EXHIBIT 2

UNITES STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

DOV ZEITLIN, individually and on behalf of all others similarly situated,

Plaintiff,

-against-

NICHOLAS PALUMBO, NATASHA PALUMBO, ECOMMERCE NATIONAL, LLC d/b/a/ Tollfreedeals.com and SIP RETAIL d/b/a sipretail.com, JON KAHEN a/k/a JON KAEN, GLOBAL VOICECOM, INC.; GLOBAL TELECOMMUNCATION SERVICES, INC. and KAT TELECOM, INC.,

Defendants.

Case No.: 1:20-cv-00510-BMC

CERTIFICATE OF SERVICE OF MOTION FOR SANCTIONS

I certify that a true and correct copy of the attached Motion and Notice of Motion, together with all attachments, exhibits, and supporting papers (viz. the notice of motion, the memorandum of law, the declaration of Theodor Bruening and the exhibits thereto) as well as the transmittal letter, were sent by first-class U.S. mail (in a properly-addressed envelope with first class postage duly paid) before 5:00 p.m. on April 11, 2020 to the attorney of record for plaintiff in this action at the address as listed below:

Robert Tolchin, Esq.
The Berkman Law Office, LLC
111 Livingston Street, Suite 1928
Brooklyn, New York 11201

The same documents were also sent as a courtesy by email as attachments to Robert Tolchin at rtolchin@berkmanlaw.com on April 10, 2020 and again on April 12, 2020 via sharefile link. On April 12, 2020, Mr. Tolchin confirmed by email that he had received the documents.

SIGNED on April 10, 2020.

/s/ Theodor Bruening
Theodor Bruening

Attorney for
Nicholas Palumbo, Natasha Palumbo,
Ecommerce National, LLC d/b/a/ Tollfreedeals.com and
Sip Retail d/b/a sipretail.com

LAW OFFICE OF THEODOR BRUENING, ESQ.

77 W 85 ST. NEW YORK NY 10024
DIRECT: (347) 403-4722
BRUENINGLAWYER@GMAIL.COM

April 10, 2020

VIA EMAIL AND USPS

Robert Tolchin, Esq.
The Berkman Law Office, LLC
111 Livingston Street, Suite 1928
Brooklyn, New York 11201
rtolchin@berkmanlaw.com

Re: *Zeitlin v. Palumbo et al.* (1:20-cv-00510)

Dear Robert:

As you know, I represent defendants Nicholas and Natasha Palumbo as well as Ecommerce National, LLC, and SIP Retail, LLC (the "defendants") in the above-referenced case. Pursuant to F.R.C.P. 11(c)(2), attached hereto is a motion for sanctions that will be filed on or after May 1, 2020. A hard copy is being mailed to your office today pursuant to F.R.C.P. 5(b)(2)(C). For the reasons stated in the motion, the complaint must be withdrawn, and the case must be discontinued with prejudice immediately, at least as to the defendants. If the complaint is withdrawn and the case is discontinued, sanctions can be avoided under F.R.C.P. 11(c)(2).

Sincerely,

Theodor Bruening

UNITES STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

DOV ZEITLIN, individually and on behalf of all others similarly situated,

Plaintiff,

-against-

NICHOLAS PALUMBO, NATASHA PALUMBO, ECOMMERCE NATIONAL, LLC d/b/a/ Tollfreedeals.com and SIP RETAIL d/b/a sipretail.com, JON KAHEN a/k/a JON KAEN, GLOBAL VOICECOM, INC.; GLOBAL TELECOMMUNCATION SERVICES, INC. and KAT TELECOM, INC.,

Defendants.

Case No.: 1:20-cv-00510-BMC

NOTICE OF MOTION

PLEASE TAKE NOTICE that, upon the accompanying declaration of Theodor Bruening, sworn to April 10, 2020 and the exhibits thereto, the memorandum of law in support of motion for sanctions, and upon all pleadings, papers, and proceedings filed in this case, defendants Nicholas Palumbo, Natasha Palumbo, Ecommerce National, LLC d/b/a/ Tollfreedeals.com and Sip Retail d/b/a sipretail.com ("defendants") will respectfully move this Court before the Hon. Brian M. Cogan at the U.S. Courthouse located at 225 Cadman Plaza East, Brooklyn, NY 11201, at a date and time to be determined by the Court, for an Order granting sanctions against plaintiff and award reasonable legal fees to defendants, pursuant to Rule 11 of the Federal Rules of Civil Procedure, on the grounds that counsel has not undertaken an independent inquiry into the facts before filing the complaint, that there is no factual or legal basis for the claims asserted in the complaint, and that plaintiff's claims were asserted for an improper purpose.

Dated: New York, New York
April 10, 2020

Theodor Bruening
Attorney for Defendants
77 W 85th Street
New York, NY 10024
BrueningLawyer@Gmail.com
(347) 403-4722

UNITES STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

DOV ZEITLIN, individually and on behalf of all others similarly situated,

Plaintiff,

-against-

NICHOLAS PALUMBO, NATASHA PALUMBO, ECOMMERCE NATIONAL, LLC d/b/a/ Tollfreedeals.com and SIP RETAIL d/b/a sipretail.com, JON KAHEN a/k/a JON KAEN, GLOBAL VOICECOM, INC.; GLOBAL TELECOMMUNCATION SERVICES, INC. and KAT TELECOM, INC.,

Defendants.

Case No.: 1:20-cv-00510-BMC

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANTS NICHOLAS PALUMBO, NATASHA PALUMBO, ECOMMERCE NATIONAL, LLC D/B/A/ TOLLFREEDEALS.COM AND SIP RETAIL D/B/A SIPRETAIL.COM'S MOTION FOR SANCTIONS

Theodor Bruening
Attorney for Defendants
77 W 85th Street
New York, NY 10024
BrueningLawyer@Gmail.com
(347) 403-4722

April 10, 2020

TABLE OF CONTENTS

Table of Authorities iv

Introduction 1

Background 2

A. The Parties 2

B. The VOIP Industry and Technology 2

C. Concurrent Proceeding Before this Court and Analysis of the Complaint 5

Argument 7

I. Legal Standard for Sanctions Under F.R.C.P. 11(b) 7

II. Counsel Has Not Undertaken a Reasonable Inquiry, and There Is No Factual Basis for the Allegations 8

A. The Timing of the Filing of the Complaint Makes an Independent Inquiry Impossible 8

B. The Contents of the Complaint Show that No Independent Inquiry Took Place 9

C. The Complaint Is Impermissibly Based Entirely on Information and Belief Pleading 11

III. There Is No Legal Basis for the Claims Asserted 12

A. Plaintiff Does Not Allege That Defendants Made Any Calls 14

B. Plaintiff Does Not Specify That He Received a Call 15

C. Plaintiff Does Not Allege That He Was Called Using an ATDS or Received a Pre-Recorded Voice Message 16

D. Plaintiff Does Not Allege That He Did Not Consent to Being Called 16

E. There Is No Case for Modifying or Extending Existing Law 16

F. Plaintiff's Complaint Warrants Sanctions 16

IV. Plaintiff's Claims Were Asserted for an Improper Purpose 17

V. An Award of Attorney's Fees Is Warranted to Cover Defendants' Legal Expenses and Deter Further Misconduct 18

Conclusion 20

TABLE OF AUTHORITIES

Cases

Barrett v F.W. Woolworth Corp.
1997 US Dist LEXIS 19277, 96 Civ. 7538 (SDNY 1997) 19

Bradgate Assocs. v. Fellows, Read & Assocs.
999 F.2d 745 (3d Cir. 1993).....10

Brown v Ameriprise Fin. Servs.
2011 US Dist LEXIS 100841, No. 09-2413 (D Minn 2011) 12

Cain v Twitter Inc.
2018 US Dist LEXIS 180942, 17-cv-02506 (ND Cal 2018) 19

Chandler v. Norwest Bank Minn., N.A.
137 F.3d 1053 (8th Cir. 1998) 8

Eastway Const. Corp. v. City of New York
762 F.2d 243 (2d Cir. 1985).....8

Foster v. Michelin Tire Corp.
108 F.R.D. 412 (C.D. Ill. 1985). 10

Garr v U.S. Healthcare
22 F3d 1274 (3d Cir 1994).....9, 11

Gjokaj v. HSBC Mortg. Servs.
2014 U.S. Dist. LEXIS 89205 (ED Mich 2014) 11

Gonzalez v County of Merced
2017 US Dist LEXIS 82402, No. 1:16-cv-01682 (ED Cal May 26, 2017) 12

Gurary v Nu-Tech Bio-Med, Inc.
303 F3d 212 (2d Cir 2002).....19

Indianapolis Colts v. Baltimore
775 F.2d 177 (7th Cir. 1985) 11

Jacques v. DiMarzio, Inc.
216 F. Supp. 2d 139 (E.D.N.Y. 2002) 17

Kaplan v Hezbollah
2020 US Dist LEXIS 31270, 19-cv-3187 (EDNY Feb. 23, 2020) 19

King v. Time Warner Cable
113 F. Supp. 3d 718 (SDNY 2015).....14, 16

Knipe v. Skinner
19 F.3d 72 (2d Cir. 1994).....18

Kropelnicki v. Siegel
290 F.3d 118 (2d Cir. 2002)..... 7-8

Mars Steel Corp. v. Continental Bank N.A.
880 F.2d 928 (7th Cir. 1989) 17

Melito v Am. Eagle Outfitters, Inc.
2015 US Dist LEXIS 160349, 14-CV-02440 (SDNY 2015).....13, 14

Miller v. Schweickart
413 F. Supp. 1059 (S.D.N.Y. 1976).....12

Mohammed v. Union Carbide Corp.
606 F. Supp. 252 (E.D. Mich. 1985).....18

Oliveri v. Thompson
803 F.2d 1265 (2d Cir. 1986).....11

Profile Publ'g & Mgmt. Corp. APS v. Musicmaker.com, Inc.
242 F. Supp. 2d 363 (S.D.N.Y. 2003).....11

Rodriguez-O'Ferral v. Trebol Motors Corp.
154 F.R.D. 33 (1st Cir. 1995) 17

Rotberg v Jos. A. Bank Clothiers, Inc.
345 F Supp 3d 466 (SDNY 2018) 16

Roundtree v. United States
40 F.3d 1036 (9th Cir. 1994) 18

Shatsky v Syrian Arab Republic
312 FRD 219 (DDC 2015).....19

Seto v. Thielen
519 Fed. Appx. 966 (9th Cir. 2013)..... 16-17

Tenay v. Culinary Teacher's Ass'n of Hyde Park, N.Y., Inc.
225 F.R.D. 483 (S.D.N.Y. 2005) 16

Townsend v. Holman Consulting Corp.
929 F.2d 1358 (9th Cir. 1990) 17

Unioil, Inc. v. E.F. Hutton & Co.
809 F.2d 548 (9th Cir. 1986) 12

United States v. Int'l Bhd. of Teamsters, Chauffeurs, Warehousemen & Helpers of Am., AFL-CIO
948 F.2d 1338 (2d Cir. 1991)..... 8-9

USA v. Palumbo, et al.
20-cv-473 .....5, 11

USA v. Kahen, et al.
1:20-cv-474 .....5, 11

Window Headquarters v MAI Basic Four
1994 US Dist LEXIS 17104, 91 Civ. 1816, 93 Civ. 4135,
92 Civ. 5283 (SDNY 1994) 12

Statutes and Rules

Fed. R. Civ. P. 11..... *passim*

47 U.S.C. § 227.....13

UNITES STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

DOV ZEITLIN, individually and on behalf of all others similarly situated,

Plaintiff,

-against-

NICHOLAS PALUMBO, NATASHA PALUMBO, ECOMMERCE NATIONAL, LLC d/b/a/ Tollfreedeals.com and SIP RETAIL d/b/a sipretail.com, JON KAHEN a/k/a JON KAEN, GLOBAL VOICECOM, INC.; GLOBAL TELECOMMUNCATION SERVICES, INC. and KAT TELECOM, INC.,

Defendants.

Case No.: 1:20-cv-00510-BMC

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANTS NICHOLAS PALUMBO, NATASHA PALUMBO, ECOMMERCE NATIONAL, LLC D/B/A/ TOLLFREEDEALS.COM AND SIP RETAIL D/B/A SIPRETAIL.COM'S MOTION FOR SANCTIONS

INTRODUCTION

Plaintiff brings this Telephone Consumer Protection Act ("TCPA") class-action, purportedly individually and on behalf of others similarly situated. The complaint (docket no. 1, "Complaint" or "Compl.") in actuality contains *no* facts identifying *any* calls received by plaintiff. Indeed, the complaint fails to allege *any* actions taken by defendants that could establish liability under the TCPA. The complaint is entirely based upon "information and belief," including facts that are indisputably within plaintiff's exclusive knowledge. The text of the Complaint and the date of its filing show that the signing attorney has not discharged his personal, nondelegable responsibility to comply with the requirements of Rule 11 before signing the Complaint and that there has been no reasonable inquiry into the contents of the pleading. Sanctions are appropriate, including an award of legal fees and dismissal of the case with prejudice.

BACKGROUND[1]

A. The Parties

Plaintiff appears to live in the Eastern District of New York (Compl. ¶ 8). It has not been alleged that he received any unwanted robocalls, other than upon information and belief (Compl. ¶ 89), nor has it been alleged that he has not consented to receiving such calls.

Defendants Nicholas and Natasha Palumbo, husband and wife, are citizens of the State of Arizona. They are the owners and principal employees of two of the defendant entities, Ecommerce National, LLC, and SIP Retail, LLC, both of which are Arizona limited liability companies which the Palumbos manage out of their residence in Paradise Valley, a suburb of Phoenix, Arizona (collectively "defendants"). During the relevant period, both companies operated switching systems that permitted them to serve as intermediary carriers of telecommunications.

B. The VOIP Industry and Technology

Historically, telephone calls were made over copper wire. A landline would connect a dialer to a center where a call would be connected by a human operator to another landline by connecting two cables. Over time, the connection center became automated, but the centralized system remained. The application of microwave and semiconductor technology resulted in dramatic changes in the infrastructure of the nation's telecommunications networks. Telephony as a monopoly utility was replaced by competition; multiple players became the rule (Bruening Decl. Ex. 5, ¶¶12-20).

With the advent of the internet and increasing ubiquity of fast, high-bandwidth glass fiber connections, it became possible to make audio (and video) connections between

[1] The relevant facts are described in the accompanying declaration of Theodor Bruening dated April 10, 2020 ("Bruening Decl.") together with the exhibits annexed thereto.

computers. This technology is known as "Voice over Internet Protocol", or "VOIP." It revolutionized the industry in ways that are still emerging, including expansion of competition by increasing the number of participants in the market. The benefits to consumers have been manifold, including cheaper long-distance and international calls, easier and cheaper conference calls, improved access to information about products and access to technical and commercial assistance, and the ability to make or answer a call from one's desk phone, computer, or cellphone using the same number, or to add videoconferencing with a press of a button (*id*.).

Importantly, VOIP also allowed smaller and mid-size companies to compete with large national phone carriers. Prior to VOIP, the barriers to entry into the telecommunications market were exceedingly high – a entrant would have own and lay cables or build a network of microwave towers, as well as operate a hub that connected calls. VOIP, however, allows small companies to enter the market at low cost; operating a VOIP company requires a fast internet connection, computer hardware (known as a "switch") and readily obtainable technical knowledge. One need not be a Ph.D. graduate of one of the great engineering universities today to become adept at operating and upgrading advanced VOIP technology (*id*.).

These companies, known as "intermediary carriers" or "wholesale carriers" do not place calls – they connect other people's calls over the Internet. A large industry of such carriers has sprung up; in the U.S., they number in the thousands; more than 1,800 such companies are registered with the FCC. Their market capitalization may amount to only a few million dollars. Since it is uncommon for carriers to operate in the entire U.S., calls are routinely routed through multiple carriers before reaching their destination; a call may go through several carriers before it is connected. This is normal and advantageous to consumers – competition between carriers for the lowest cost to connect calls is robust (*id*.).

Due to differences in the internet infrastructure in different locations, carrier A might pay carrier B to connect its calls (carrier A is carrier B's "client") while at the same time carrier A might receive money from carrier B to connect calls in the other direction (carrier A is carrier B's "vendor"). It is common for carriers to be both vendors to and clients of each other (*id.*).

Intermediary carriers, like defendants, using the technology involved here do not have the ability to know if their connecting carrier or source is a foreign country or the United States (*id.*).

By their very nature, VOIP carriers are almost always far removed from the original caller or the eventual recipient of telecommunications carried on their systems. A carrier often connects a call that was originated several prior carriers earlier (i.e., the caller may typically be his client's client's client's client) and that is connected to the recipient several carriers later (i.e., the recipient may turn out to be his vendor's vendor's vendor's vendor). The content of these calls is completely unknown to the carrier. Most gateway carriers do not have access to call content, even if it were lawful to pry into such matters. A carrier such as those at issue here, therefore, has little to no control or knowledge over what calls go through his system, and little to no knowledge of the messages of calls that he connects (*id.*).

In short, fraudulent calls can be transmitted using any kind of carrier without the carriers being aware at the time that the calls are improper.

Intermediary carriers are the conduits of communications, not their source or destination. Defendants have not, and do not *place* or *make* or *initiate* any automated calls to anyone. They and their companies provide conduits for phone calls. The TCPA has never before been held to apply to VOIP carriers who do not themselves place any calls. There are good reasons why this approach has never previously been attempted. It's because defendants are

innocent service providers; to hold them responsible for the actions of others in the way requested here is contrary to the express purpose of the TCPA; it would also be overreaching and wrongly interfere with socially valuable services.

C. Concurrent Proceeding Before this Court and Analysis of the Complaint

On January 28, 2020, the U.S. Department of Justice commenced an action against defendants for injunctive relief under *inter alia* 18 U.S.C. 1345, essentially arguing that defendants did not act sufficiently when they responded to complaints concerning automated fraudulent robocalls (*USA v. Palumbo, et al.*, 20-cv-473, the "Government action"). The claim has been wholly denied by defendants (*USA v. Palumbo*, docket no. 35). There has been no exchange of discovery (beyond automatic disclosures pursuant to F.R.C.P. 26(a)(1)(A)) in that case and no finding of liability.

On that same day, the government also filed a similar action (*USA v. Kahen, et al.*, 1:20-cv-474, the "Kahen action") against Jon Kahen a/k/a Jon Kaen, Global Voicecom, Inc.; Global Telecommuncation Services, Inc. and Kat Telecom, Inc., i.e. the other defendants in the instant lawsuit.

The very next day, on January 29, 2020, plaintiff filed the instant action. On review of the Complaint, (Bruening Decl. Ex. 1) it is evident that Mr. Tolchin, plaintiff's attorney, copied the entirety of the facts alleged *verbatim* from the complaints in the Government action and in the Kahen action. Each paragraph containing any kind of alleged factual information is copied directly from the Government action and the Kahen action with the additional text: "upon information and belief."

The following paragraphs have been pleaded upon information and belief:

- Every paragraph in the section headed "The Underlying Facts" (i.e. paragraphs 25-83);

- The paragraphs describing the defendants (paragraphs 9-15);
- The first paragraph in the section of the Complaint allegedly describing the harm to the alleged victims (paragraph 84);
- The only paragraph describing anything relating to calls to the plaintiff (paragraph 89).

The paragraphs that have not been pled on information and belief either do not discuss the facts at all or do so in a highly unspecific way:

a. Paragraphs 1-5 discuss the issue of unwanted robocalls and their impact on society on an abstract level with no reference to the parties or the law;
b. Paragraph 6 makes vague claims that defendants are somehow responsible for robocalls, offering no specifics beyond claiming that defendants "facilitated" robocalls;
c. Paragraph 7 states that plaintiff hopes to stop defendants through this class-action;
d. Paragraph 8 states that plaintiff is a resident of this Court's district;
e. Paragraphs 16-17 concern jurisdiction;
f. Paragraphs 18-24 are boilerplate class action allegations;
g. Paragraph 87 refers to the two actions commenced by the Government;
h. Paragraph 88 repeats and re-alleges each of the foregoing allegations;
i. Paragraphs 90-96 are boilerplate TCPA and class action allegations without any specificity.

In short, out of 96 paragraphs, 66 paragraphs are alleged "upon information and belief" while the remaining 30 paragraphs contain boilerplate statements and legal conclusions.

Defendants have compared the complaint to the pleading in the government action. A redlined comparison document is annexed as Exhibit 4 to the declaration of Theodor Bruening submitted herewith. As shown therein, paragraphs 9-11, 25-35, 37-51, and 76-86 were copied from the Government action pleading, while paragraphs 12-15, 36, and 52-75 were copied from the *Kahen* action complaint.

ARGUMENT

I. Legal Standard for Sanctions Under F.R.C.P. 11(b)

Rule 11 of the federal Rules of Civil Procedure provides, in pertinent part, that in presenting any document to the court, an attorney certifies that to the best of his or her knowledge, information, and belief, the document is not being filed for an improper purpose; the claims are warranted by existing law; and the factual contentions have evidentiary support. Fed. R. Civ. P. 11(b). If, after notice and a reasonable opportunity to respond, the court determines that Rule 11(b) has been violated, the court has discretion to impose sanctions on the attorneys, law firms, or parties responsible for the violation. Fed. R. Civ. P. 11(c)(1).[2]

A pleading violates Rule 11 either when it "has been interposed for any improper purpose or where, after reasonable inquiry, a competent attorney could not form a reasonable belief that the pleading is well grounded in fact and is warranted by existing law or good faith argument for the extension, modification or reversal of existing law" *Kropelnicki v. Siegel*, 290

[2] Fed. R. Civ. P. 11(b) reads as follows:
Representations to the Court. By presenting to the court a pleading, written motion, or other paper—whether by signing, filing, submitting, or later advocating it—an attorney or unrepresented party certifies that to the best of the person's knowledge, information, and belief, formed after an inquiry reasonable under the circumstances:
(1) it is not being presented for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation;
(2) the claims, defenses, and other legal contentions are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law;
(3) the factual contentions have evidentiary support or, if specifically so identified, will likely have evidentiary support after a reasonable opportunity for further investigation or discovery; and
(4) the denials of factual contentions are warranted on the evidence or, if specifically so identified, are reasonably based on belief or a lack of information.

F.3d 118, 131 (2d Cir. 2002). Compliance is measured by an objective standard: Rule 11 is violated "where it is patently clear that a claim has absolutely no chance of success." *Eastway Const. Corp. v. City of New York*, 762 F.2d 243, 254 (2d Cir. 1985). Objectively, Mr. Tolchin's pleading fails all these hurdles – there was no proper purpose, no reasonable inquiry, no grounding in fact or law, no argument for modification of existing law, and no chance of success.

II. Counsel Has Not Undertaken a Reasonable Inquiry, and There Is No Factual Basis for the Allegations

A. The Timing of the Filing of the Complaint Makes an Independent Inquiry Impossible

The Complaint was filed within one day of the filing of the two government actions which undoubtedly prompted the filing of the Complaint. There was no reason for this rush – no statute of limitations was about to expire, and the Complaint does not allege any need for emergency action. Nor does a single word in the pleading show that the plaintiff received any improper calls through defendants' system; this critical factual requirement does not seem to have been considered or explored. It is not plausible that within one day Mr. Tolchin made any kind of investigation – let alone a reasonable investigation – into the veracity or sufficiency of the claims that he was asserting over 96 paragraphs in 31 pages.

Where an attorney "could not have conducted the inquiry necessary to support" their clients' claims before filing a complaint, sanctions are warranted. *Chandler v. Norwest Bank Minn., N.A.*, 137 F.3d 1053 (8th Cir. 1998), *reh'g, en banc, denied*, 1998 U.S. App. LEXIS 8504 (8th Cir. 1998), *cert. denied*, 525 U.S. 922 (1998). Nor is there any reason to permit this lacuna to be remedied through discovery since "[p]leadings, motions, and other papers must be justifiable at the time they are signed" (*United States v. Int'l Bhd. of Teamsters, Chauffeurs,*

Warehousemen & Helpers of Am., AFL-CIO, 948 F.2d 1338, 1344 (2d Cir. 1991)). Nor was there any reason to rush filing.[3]

B. The Contents of the Complaint Show that No Independent Inquiry Took Place

Several items in the complaint make it plain that Mr. Tolchin made no effort to review the pleading that he filed or ascertain its accuracy. For instance, at paragraph 38, the complaint states that "Upon information and belief, the FAQs on the TollFreeDeals website state, 'Do you handle CC (Call Center)/Dialer Traffic? Yes…'" At the time of the filing of the Complaint, the website was still online. Plaintiff could have confirmed its contents directly but did not undertake this most basic exercise in confirming the veracity of his pleadings, instead relying entirely on second-hand information.

For another example, counsel for plaintiff evidently did not draft the complaint himself but only copied-and-pasted its contents without so much as proofreading. At paragraph 50, the complaint states "from May 2019 tluough January 2020" (emphasis added). This is no ordinary typo. The complaint in the government action was filed in PDF format on PACER (as is usual). To be able to copy and paste the language from the complaint to another document, the PDF has to be reversed into a word document or similar word processor using a technology called optical character recognition ("OCR"). OCR is not perfect; sometimes "through" is recognized as "tluough" because the optical lines "hr" are similar to "lu" – one long line and two short lines. This is evidently what happened here, no one who wanted to type "through" would type "thuough" by accident, the keyboard letters are too far apart. Compare government action paragraph 34 (Bruening Decl. Ex. 2). Similar OCR typos exist at:

[3] "[A] factor in ascertaining the reasonableness of the signer's inquiry is the amount of time available to investigate the facts and law involved." *Garr v U.S. Healthcare*, 22 F3d 1274, 1279 (3d Cir 1994).

- Paragraph 79 ("fi·audulent"), compare to paragraph 41 in the government action ("fraudulent").
- Paragraph 82 ("Unfmiunately"), compare to paragraph 43 in the government action ("Unfortunately").
- Paragraph 47 ("traceback pmial"), compare to paragraph 34 in the government action ("traceback portal").

Further, some of the copying and pasting led to absurd results. Plaintiff claims in paragraph 86 that "Defendants' fraudulent schemes are ongoing and wide-ranging. Absent injunctive relief by this Court, the Defendants will continue to cause injury to victims in this District and throughout the United States, and the victims' losses will continue to mount." The paragraph makes no sense in the current action in which plaintiff is not requesting injunctive relief. The paragraph is also not preceded by the phrase "upon information and belief," which means that counsel must have an actual, reasonable, personal and non-derivative basis for making the allegation that defendants engage in "ongoing and wide-ranging" fraudulent schemes.

In determining whether Rule 11 has been violated, the focus of a court's inquiry should be the reasonableness of the investigation undertaken, not whether the moving party was prejudiced by the actions of the party under scrutiny. *Bradgate Assocs. v. Fellows, Read & Assocs*., 999 F.2d 745 (3d Cir. 1993). Counsel's inquiry cannot be described as reasonable by any definition of that term.[4]

[4] Indeed, courts have drawn a distinction between Rule 11 and Rule 12(b)(6); a plaintiff may have reasonable claim, indeed an irrefutable claim, an assertion of which may nonetheless violate Rule 11 if he has failed to conduct any reasonable inquiry. *Foster v. Michelin Tire Corp*., 108 F.R.D. 412 (C.D. Ill. 1985).

C. The Complaint Is Impermissibly Based Entirely on Information and Belief Pleading

Under Rule 11(b), an attorney who presents a pleading, written motion, or other paper with the court certifies that to the best of his or her knowledge, formed after an inquiry reasonable under the circumstances, the allegations and other factual contentions contained in it have evidentiary support.

Here, Counsel's entire complaint is impermissibly based on "upon information and belief" pleading. The entire text of the factual allegations is an identical copy of the facts alleged in the complaints filed in *USA v. Palumbo, et al.*, EDNY case no. 20-cv-473 (Bruening Decl. Ex. 2), and *USA v. Kahen, et al.*, EDNY case no. 20-474 (Bruening Decl. Ex. 3). *See Gjokaj v. HSBC Mortg. Servs*., 2014 U.S. Dist. LEXIS 89205, *18 (ED Mich 2014) (noting that the filing of "'cookie cutter' pleadings is potentially sanctionable conduct"), *Garr v U.S. Healthcare*, 22 F3d at 1278 (the signing attorney has a "'personal, nondelegable responsibility' to comply with the requirements of Rule 11 before signing the document" including "a reasonable inquiry into the contents of the pleading.").

Rule 11 requires a careful investigation and consideration of claims asserted and inclusion of boilerplate allegations is improper and subject to appropriate sanctions. *Oliveri v. Thompson*, 803 F.2d 1265, 1280 (2d Cir. 1986), *cert. denied*, 480 U.S. 918 (1987). The question of reasonableness is an objective one, not based on the filing attorney's subjective belief. *Indianapolis Colts v. Baltimore*, 775 F.2d 177 (7th Cir. 1985). A failure to conduct a reasonable inquiry warrants sanctions. *Profile Publ'g & Mgmt. Corp. APS v. Musicmaker.com, Inc*., 242 F. Supp. 2d 363 (S.D.N.Y. 2003).

Indeed, given the paucity of detail concerning the call(s) received by the lead plaintiff – information exclusively in the possession of the plaintiff – it is questionable whether

counsel ascertained whether Mr. Zeitlin's claims are typical of the class and if he would fairly and adequately protect the interests of the class. A failure to make this determination is sanctionable conduct under Rule 11. *Unioil, Inc. v. E.F. Hutton & Co.*, 809 F.2d 548 (9th Cir. 1986), *cert. denied*, 484 U.S. 822 (1987), *see also Garr v. U.S. Healthcare*, 22 F.3d 1274 (3d Cir. 1994), *reh'g, en banc, denied*, 1994 U.S. App. LEXIS 16425 (3d Cir. 1994).

Nor is it sufficient to point to the government action and plead the exact same facts upon information and belief. Lawyers have a responsibility before subscribing their names to complaints which contain serious charges to ascertain that reasonable basis in fact exists for allegations contained in the pleadings, even if they are made upon information and belief. *Miller v. Schweickart*, 413 F. Supp. 1059 (S.D.N.Y. 1976). *See also Gonzalez v County of Merced*, 2017 US Dist LEXIS 82402, at *18, n 8, No. 1:16-cv-01682 (ED Cal May 26, 2017) (noting that "information and belief" pleading does not grant immunity from sanctions), *see also Window Headquarters v MAI Basic Four*, 1994 US Dist LEXIS 17104, at *53-55, 91 Civ. 1816, 93 Civ. 4135, 92 Civ. 5283 (SDNY 1994), *Brown v Ameriprise Fin. Servs.*, 2011 US Dist LEXIS 100841, at *7, No. 09-2413 (D Minn 2011) (copying and pasting factual assertions from an unrelated complaint violates Rule 11).

Nor is there any compliance with F.R.C.P. 11(b)(3), which allows for pleading where the factual contentions "if specifically so identified, will likely have evidentiary support after a reasonable opportunity for further investigation or discovery" since plaintiff has not identified *any* facts which if reviewed in discovery would sustain his claim.

III. There Is No Legal Basis for the Claims Asserted

In addition to the issues concerning the purported factual basis for the complaint, this court should exercise its discretion to sanction counsel for filing a lawsuit for which there was clearly no legal basis. It is well established that only persons and entities that originate

phone calls are liable under the TCPA. *Melito v Am. Eagle Outfitters, Inc.*, 2015 US Dist LEXIS 160349, 14-CV-02440 (SDNY 2015).

A responsible pre-filing inquiry into the TCPA case law would have revealed to counsel that (1) the statute does not provide for a cause of action against an intermediary VOIP carrier and that (2) that the elements of a TCPA claim are not supported by the facts asserted in the complaint.

Plaintiff alleges that Defendants violated the TCPA, though it is unclear which provision of the TCPA was allegedly violated. The Complaint only refers to 47 U.S.C. § 227 (Compl. ¶ 90) and to "TCPA" generally (Compl. ¶¶ 90, 91, 93). Presumably, plaintiff refers to 47 U.S.C. § 227(b)(1)(A)(iii) and (b)(3),[5] which provide a private cause of action for unwanted robocalls.

---

[5] The relevant TCPA provisions read as follows:

47 U.S.C. § 227 (b)

(1) Prohibitions. It shall be unlawful for any person within the United States, or any person outside the United States if the recipient is within the United States—

(A) to make any call (other than a call made for emergency purposes or made with the prior express consent of the called party) using any automatic telephone dialing system or an artificial or prerecorded voice—

…

(iii) to any telephone number assigned to a paging service, cellular telephone service, specialized mobile radio service, or other radio common carrier service, or any service for which the called party is charged for the call, unless such call is made solely to collect a debt owed to or guaranteed by the United States;

…

(3) Private right of action. A person or entity may, if otherwise permitted by the laws or rules of court of a State, bring in an appropriate court of that State—

(A) an action based on a violation of this subsection or the regulations prescribed under this subsection to enjoin such violation,

(B) an action to recover for actual monetary loss from such a violation, or to receive $500 in damages for each such violation, whichever is greater, or

(C) both such actions.

If the court finds that the defendant willfully or knowingly violated this subsection or the regulations prescribed under this subsection, the court may, in its discretion, increase the amount of the award to an amount equal to not more than 3 times the amount available under subparagraph (B) of this paragraph.

"To make out a claim under the TCPA, [a plaintiff] must show that (1) (a defendant) called her on her cell phone; (2) using an automated telephone dialing system ["ATDS"] or pre-recorded voice; (3) without her consent." *King v. Time Warner Cable*, 113 F. Supp. 3d 718, 725 (SDNY 2015), *rev'd on other grounds*, 894 F.3d 473 (2d Cir. 2018). The Complaint fails to allege facts supporting any of these elements.

A. Plaintiff Does Not Allege That Defendants Made Any Calls.

Only the person who physically "makes" or "initiates" a call within the meaning of the TCPA can be subject to direct TCPA liability. *See, e.g.*, *Melito*, 2015 WL 7736547, at *4-5. Thus, federal courts routinely reject direct TCPA claims lacking sufficient facts regarding "the making, or physical placement" of a phone call. *Id.* Plaintiff concedes that Defendants did not *make* or *place* the calls: the Complaint claims defendants "facilitated" (Compl. ¶¶ 5, 41), "transmit" (id. ¶¶ 26(a)-(e), 35, 36, 40, 57, 61), and "deliver" (id, ¶ 42) robocalls and that they "serve[d] as a gateway carrier", (id. ¶¶ 31, 33, 34), "provided U.S.-bound calling services" (id. ¶34), "pass[ed] robocalls into the U.S. telephone system" (id. ¶¶ 34, 63, 76), "provide[d] inbound VoiP calling" (id. ¶ 37), "market[d] their services to foreign call centers" (id. ¶ 38), and "provide[d] return-calling services" (id. ¶ 66). That is the sum total of the allegations against defendants. Plaintiff nowhere alleges that defendants were instrumental in the *placement* of any call. Plaintiff only – correctly – asserts that defendants were conduits for calls. If that were sufficient to impose liability under the TCPA, then Verizon and AT&T would be equally liable for robocalls travelling through their networks as would any person laying phone lines.

Purported class plaintiff claims only *once* in the entire Complaint that defendants "placed" a call to plaintiff – at the very end, in the first cause of action, after the narrative of facts. The allegation is made in the most unspecific way possible:

> The plaintiff, and each member of the proposed plaintiff class, has received numerous robocalls which, upon information and belief, were carried, processed, connected, ***placed***, routed, and/or facilitated by the defendants and/or the agents, servants, employees, and related entities.
> (Compl. ¶ 89, emphasis added)

That's it. [6] Plaintiff does not, and cannot, point to a single call received by plaintiff placed by defendants. Similarly, plaintiff does not, and cannot, provide the number of a call received by him, or the date and time of such a call, or the call contents, or that any such call was in any way connected to defendants.

Plaintiff variously claims that defendants were involved in a conspiracy with the entities placing the calls, e.g. Compl. ¶¶ 31 (referring to "Defendants' robocalling fraud scheme"), 41 (referring to an alleged "co-conspirator"). Plaintiff has not alleged any facts supporting any such relationship beyond the barest conclusory assertions, averred "upon information and belief." If anything, plaintiff's claims amount to an assertion that defendants did not do enough to stop robocalls travelling through their VOIP switch when alerted to this fact by third parties. The TCPA does not recognize this as a basis for liability in private lawsuits; nor has any court in the U.S. taken this position.

B. Plaintiff Does Not Specify That He Received a Call

Throughout the Complaint, plaintiff *nowhere* states when he received a robocall, or how many he received, or from which number he received calls, or what the robocalls stated, or what makes him believe that defendants placed the calls. The Complaint merely states that "plaintiff, and each member of the proposed plaintiff class, has received numerous robocalls which, *upon information and belief*, were carried, processed, connected, placed, routed, and/or

[6] In addition, it is likely that, taken in context, the word "placed" here is not intended to connote the person making a call – in the sense of causing it – but rather means someone who connects or routes the call.

facilitated by the defendants…" (Compl. ¶ 89, emphasis added). No plausible allegations are presented that would tie defendants, among 1,800 intermediary carriers in the United States, to even one of the calls claimed to be received by plaintiff.

C. Plaintiff Does Not Allege That He Was Called Using an ATDS or Received a Pre-Recorded Voice Message

Plaintiff does not allege anywhere that he was called using an ATDS as required by the statute (*see King supra*), or that defendants used an ATDS, or that he received a prerecorded voice message. Plaintiff claims throughout – and only "upon information and belief" – that persons *other than plaintiff* received automated or pre-recorded voice calls that were routed *through* defendants' system (e.g. Compl. ¶¶ 46, 47, 56). The absence of this assertion is fatal to plaintiff's claim.

D. Plaintiff Does Not Allege That He Did Not Consent to Being Called

It is a basic requirement that lack of consent to be called has to be pled in a TCPA case. *Rotberg v Jos. A. Bank Clothiers, Inc.*, 345 F Supp 3d 466 (SDNY 2018). Plaintiff nowhere argues that any calls received by him – placed by defendants or anyone else – were received without his consent.

E. There Is No Case for Modifying or Extending Existing Law

Plaintiff has not argued that the current TCPA liability should be extended to intermediary VOIP carriers and no basis for such an argument exists.

F. Plaintiff's Complaint Warrants Sanctions

The law is settled that a failure to research and apply federal law in an action brought in federal court warrants sanctions where the failure causes the other party to incur unnecessary costs. *Tenay v. Culinary Teacher's Ass'n of Hyde Park, N.Y., Inc.*, 225 F.R.D. 483 (S.D.N.Y. 2005), *aff'd*, 281 Fed. Appx. 11 (2d Cir. 2008), *see also Seto v. Thielen*, 519 Fed.

Appx. 966 (9th Cir. 2013). An attorney may not pretend that the law favors his view and impose on court or his adversaries the burden to research and uncover basic rules of the law; attorneys who do so are properly sanctioned. *Mars Steel Corp. v. Continental Bank N.A.*, 880 F.2d 928 (7th Cir. 1989).

A failure to state all the necessary elements of a claim is grounds for sections. *Rodriguez-O'Ferral v. Trebol Motors Corp.*, 154 F.R.D. 33, *aff'd*, 45 F.3d 561 (1st Cir. 1995) (sanctions imposed on plaintiffs' attorneys who utterly failed his responsibility to investigate and evaluate the facts prior to filing complaint which did not state all necessary elements to support the allegations.). A failure to research the law prior to the filing of a complaint warrants sanctions. *Frank v D'Ambrosi* (1993, CA6 Ohio) *app dismd* 1994 US App LEXIS 15187 (CA6 Mich). A complaint devoid of allegations rising to colorable claim for any of the legal theories asserted also warrants sanctions. *Jacques v. DiMarzio, Inc.*, 216 F. Supp. 2d 139 (E.D.N.Y. 2002).

IV. Plaintiff's Claims Were Asserted for an Improper Purpose.

Because essential baseline facts are indisputable and because the law is so clearly against him, the only reasonable inference to be drawn is that the complaint was filed solely for the improper purpose of oppressing defendants and forcing a settlement.

A party who files a pleading for an improper purpose, such as harassing or punishing the opposing party, violates Rule 11(b)(1) and may therefore be sanctioned. The test for whether a party acted with an improper purpose is objective—that is, whether the party's outward behavior manifested an improper purpose. *Townsend v. Holman Consulting Corp.*, 929 F.2d 1358, 1366 (9th Cir. 1990) (en banc). A court may infer from "solid evidence of a pleading's frivolousness" that a pleading was filed for an improper purpose. *Id.* at 1365.

In the present case, there is no objective excuse or reason to file a complaint such as the one at bar. It does not meet *any* of the elements required for the alleged cause of action and is *entirely* based on secondhand knowledge with *no* apparent independent investigation. Mr. Tolchin's frivolous and cavalier conduct warrants dismissal of the action with prejudice and the imposition of sanctions.

D. An Award of Attorney's Fees Is Warranted to Cover Defendants' Legal Expenses and Deter Further Misconduct

This Court may exercise its discretion to impose sanctions against both plaintiff and his attorneys for their violations of Rule 11(b). *Roundtree v. United States*, 40 F.3d 1036, 1040 (9th Cir. 1994). Any attorney signing pleadings is obligated under Rule 11 to refrain from raising claims without first conducting reasonable inquiry into the underlying facts and law on which those claims are predicated; the "reasonable inquiry" standard at very least requires some kind of investigation, and some affirmative conduct on part of the attorney. The attorney is also obligated to dissuade his client from pursuing specious claims. *Mohammed v. Union Carbide Corp*., 606 F. Supp. 252 (E.D. Mich. 1985).

Rule 11 sanctions are to be imposed with caution, *Knipe v. Skinner*, 19 F.3d 72, 78 (2d Cir. 1994), and should be limited to those sanctions necessary to deter the offender and those similarly situated from engaging in similar conduct. F.R.C.P. 11(c)(4). In determining whether to impose sanctions, the court may consider the following factors, among others: (1) whether the improper conduct was willful, or negligent; (2) whether it was part of a pattern of activity, or an isolated event; (3) whether it infected the entire pleading, or only one particular count or defense; (4) whether the person has engaged in similar conduct in other litigation; (5) whether it was intended to injure; and (6) what effect it had on the litigation process in time or

expense. Fed. R. Civ. P. 11, advisory committee notes of 1993. Applying the above factors, it is clear that sanctions are appropriate in the present case:

(1) The misconduct of counsel was clearly willful, as he must have known that his inquiry into the facts and the law of the matter was so scant as to be nonexistent.

(2) and (4), counsel is no stranger to having his claims dismissed as baseless and receiving warnings from judges – this Court and other courts have frequently dismissed his complaints for various reasons and excoriated counsel, *see e.g. Kaplan v Hezbollah*, 2020 US Dist LEXIS 31270, 19-cv-3187 (EDNY Feb. 23, 2020), Cogan J. (dismissing case), *see also Cain v Twitter Inc.*, 2018 US Dist LEXIS 180942, 17-cv-02506 (ND Cal 2018) (dismissing case), *Shatsky v Syrian Arab Republic*, 312 FRD 219 (DDC 2015) (sanction of preclusion of documents), *see also Gurary v Nu-Tech Bio-Med, Inc.*, 303 F3d 212 (2d Cir 2002) (Mr. Tolchin's co-counsel was sanctioned under Rule 11(b) for bringing frivolous claims), *Barrett v F.W. Woolworth Corp.*, 1997 US Dist LEXIS 19277, 96 Civ. 7538 (SDNY 1997) (finding monetary sanctions appropriate in situations where "attorneys, such as Mr. Tolchin here, fail to follow" court orders).

(3) As plaintiff's complaint, consisting of a single count, is wholly groundless from its inception, the misconduct in this case infected the entire pleading and was the direct cause of all of the expenses incurred by defendants in this litigation.

(5) Finally, the very nature of the misconduct—filing a groundless complaint with no factual or legal basis—makes it clear that counsel acted with the improper purpose of using the courts to extract a costly settlement knowing that the defense of a class action would be expensive.

In short, the conduct was precisely the type of egregious abuse of the legal process that Rule 11 sanctions were designed to deter.

Appropriate sanctions in this case should include an award of the total amount of reasonable attorney's fees and expenses incurred by defendants in defending this case. Without an award of fees, plaintiff will have achieved its goal of groundlessly harassing defendants. Thus, an award of reasonable attorney's fees to defendants is necessary to deter counsel's continued filing of unconsidered lawsuits. See Fed. R. Civ. P. 11(c).

CONCLUSION

For the reasons described above, the Defendants' Motion to for Sanctions should be granted.

Dated: New York, New York
April 10, 2020

By: _____
Theodor Bruening

Attorney for Defendants
77 W 85th Street
New York, NY 10024
BrueningLawyer@Gmail.com
(347) 403-4722

UNITES STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

DOV ZEITLIN, individually and on behalf of all others similarly situated,

Plaintiff,

-against-

NICHOLAS PALUMBO, NATASHA PALUMBO, ECOMMERCE NATIONAL, LLC d/b/a/ Tollfreedeals.com and SIP RETAIL d/b/a sipretail.com, JON KAHEN a/k/a JON KAEN, GLOBAL VOICECOM, INC.; GLOBAL TELECOMMUNCATION SERVICES, INC. and KAT TELECOM, INC.,

Defendants.

Case No.: 1:20-cv-00510-BMC

DECLARATION OF THEODOR BRUENING

THEODOR D.E. BRUENING, hereby declares pursuant to 28 U.S.C. § 1746 as follows:

1. I am counsel to defendants Nicholas Palumbo, Natasha Palumbo, Ecommerce National, LLC d/b/a/ Tollfreedeals.com and Sip Retail d/b/a sipretail.com (hereinafter "Palumbo Defendants"), in this action. I submit this declaration in support of defendants' motion for sanctions.

2. A copy of the complaint filed in docket no. 1 in this action is annexed hereto as Exhibit 1 (the "Complaint" or "*Zeitlin* Complaint").

3. A copy of the complaint filed in *USA v. Palumbo, et al*. 20-cv-473 is annexed hereto as Exhibit 2.

4. A copy of the complaint filed in *USA v. Kahen, et al*. 20-cv-474 is annexed hereto as Exhibit 3.

5. I used Microsoft Word to create a comparison document showing the extent to which text from *USA v. Palumbo, et al*. was used in the *Zeitlin* Complaint. The resulting document is annexed hereto as Exhibit 4. In Exhibit 4, text that is formatted "normally" is present *verbatim* in both documents. Underlined text (like this) is present in in the *Zeitlin* Complaint, but not in the *USA v. Palumbo* complaint. Crossed-out text (~~like this~~) is present in the *USA v. Palumbo* complaint, but not in the *Zeitlin* Complaint.

6. A review of Exhibit 4 and of the complaints in *USA v. Palumbo* and *USA v. Kahen* shows that:

a. The material facts relating to the Palumbo Defendants in the *Zeitlin Complaint* have been copied *verbatim* from the *USA v. Palumbo* complaint; and

b. The material facts relating to the remaining defendants have been copied *verbatim* from the *USA v. Kahen* complaint (in Exhibit 4 those parts show as underlined since Exhibit 4 only compares the *Zeitlin* Complaint with the *USA v. Palumbo* complaint; however a review of the *USA v. Kahen* complaint shows that all paragraphs relating to those complaints (including ¶¶ 12-15, 36, 52-75) were taken *verbatim* from the text in the *USA v. Kahen* complaint).

7. A copy of the declaration of Nicholas filed in *USA v. Palumbo, et al*. 20-cv-473 (docket no. 38) is annexed hereto as Exhibit 5.

Dated: New York, New York
April 10, 2020

Theodor Bruening

EXHIBIT 1

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------X

DOV ZEITLIN, individually and on behalf of all others similarly situated,

Plaintiff,

-against-

NICHOLAS PALUMBO; NATASHA PALUMBO; ECOMMERCE NATIONAL, LLC d/b/a TollFreeDials.com; SIP RETAIL d/b/a sipretail.com; JON KAHEN a/k/a JON KAEN; GLOBAL VOICECOM, INC.; GLOBAL TELECOMMUNCATION SERVICES, INC.; and KAT TELECOM, INC.,

Defendants.

----------X

Case no.
20-cv-510

COMPLAINT

Jury trial demanded

Plaintiff, complaining of the defendants, by his attorneys, THE BERKMAN LAW OFFICE, LLC, alleges for his complaint, upon information and belief, as follows:

INTRODUCTION

1. The phenomenon of robocalls has become a scourge plaguing our society.

2. For years Americans have been constantly bombarded with robocalls seeking to draw them into all manner of fraudulent schemes with lies and deceit. Call recipients are told that their social security numbers will be "frozen" if they do not cooperate with a bogus investigator who needs money to be sent in immediately, that they will be arrested for money laundering or drug dealing, that they must provide their credit card or banking information, that their car warranties are about to expire, that they need to provide credit card information for cockeyed

reasons, that there are tax liens against them, that they are going to be deported, and the list goes on. Many have been bombarded with pointless calls playing recordings in Chinese, Spanish, and other foreign languages they do not even speak.

3. The problem has become so severe that in 2018 when the Swedish Royal Academy of Sciences called New York University professor Paul Romer to inform him that he had won the Nobel Prize in Economics, he let the call go to voicemail thinking that only a telemarketing call could be coming in at such an early hour. He told the media "I didn't answer the phone because I've been getting so many spam calls. I just assumed it was more spam."

4. Millions of Americans have had their children woken up, had their dinner hour disturbed, have their work interrupted, have been unable to keep their phones on so their families could reach them for fear of having it ring at an inopportune time, have had to put important calls on hold to answer what turns out to be a spam robocall, and have otherwise have had their lives made miserable by spam robocalls.

5. The Defendants in this case are responsible for this scourge. Disregarding all laws, ignoring complaints and warnings, and acting with a selfish quest for mammon regardless of the intrusive burden they placed on their fellow Americans, the Defendants deliberately facilitated hundreds of millions of spam robocalls, while hiding behind false telephone numbers and spoofed caller ID's.

6. In this action, plaintiff seeks justice on his own behalf, and on behalf of all the Defendants' other victims.

7. It is the plaintiff's hope that by imposing a financial cost on the defendants for the wanton aggravation they have caused to millions of Americans, the profit motive will be

eliminated, similar conduct by others will be deterred, and Americans' quality of life can be improved.

THE PARTIES

8. At all times relevant to this complaint, the plaintiff, DOV ZEITLIN ("ZEITLIN"), is a natural person, resident of the State of New York, County of Kings.

9. Upon information and belief, at all times relevant to this complaint, Defendants Nicholas and Natasha Palumbo own and control Ecommerce National, LLC, doing business as TollFreeDeals.com and SIP Retail, LLC, also doing business as SipRetail.com (the "Palumbo Corporate Defendants"), which the Palumbos utilize in furtherance of the fraudulent robocall schemes. The Palumbos operate the Corporate Defendants from their home in Paradise Valley, Arizona, and on information and belief, the Palumbos operate SIP Retail as an alter ego of Ecommerce. From their home in Paradise Valley, Arizona, the Palumbos operate the Corporate Defendants as fraudulent enterprises.

10. Upon information and belief, at all times relevant to this complaint, Defendant Ecommerce is a corporation organized and existing under the laws of the State of Arizona. Ecommerce does business as TollFreeDeals.com, and will be referred to throughout this Complaint as TollFreeDeals. TollFreeDeals' principal place of business is located at the Palumbos' home in Paradise Valley, Arizona. Nicholas Palumbo is the Chief Executive Officer of TollFreeDeals and Natasha Palumbo is the Vice President of Business Development.

11. Upon information and belief, at all times relevant to this complaint, Defendant SIP Retail, LLC, also doing business as SipRetail.com ("SIP Retail"), is a corporation organized and existing under the laws of the State of Arizona. SIP Retail's principal place of business is located at the Palumbos' home in Paradise Valley, Arizona. Natasha Palumbo is the Chief Executive Officer of SIP Retail. SIP Retail provides VoiP carrier services for some of the same customers as

TollFreeDeals, including foreign VoiP carriers that transmit millions of calls every week destined for the phones of residents of the Eastern District of New York.

12. Upon information and belief, at all times relevant to this complaint, Defendant Kaen resides in Nassau County, New York, in the Eastern District of New York. Kaen controls Defendants Global Voicecom, Inc., Global Telecommunication Services Inc., and KAT Telecom, Inc., which he uses in furtherance of the fraudulent robocall scheme. Kaen operates the Corporate Defendants as a single enterprise from his home in the Eastern District of New York. One or more of these Defendants also conducts business as "IP Dish."

13. Upon information and belief, at all times relevant to this complaint, Defendant Global Voicecom, Inc. is a New York corporation. The New York Department of State, Division of Corporations Entity Information database identifies Global Voicecom's principal executive office as being located in Great Neck, New York, in the Eastern District of New York, and Kaen as the corporation's Chief Executive Officer.

14. Upon information and belief, at all times relevant to this complaint, Defendant Global Telecommunication Services Inc. is a New York corporation. Global Telecommunication Service's principal place of business is located in Great Neck, New York, in the Eastern District of New York.

15. Upon information and belief, at all times relevant to this complaint, Defendant KAT Telecom, Inc. is a New York corporation. KAT Telecom's principal place of business is located in Great Neck, New York, within the Eastern District of New York.

JURISDICTION

16. This court has jurisdiction over this action pursuant to 28 U.S.C. § 1331, 47 U.S.C. § 227, as well as 28 U.S.C. § 1367.

17. Venue lies in this district pursuant to 28 U.S.C. § 1391(b)(2)

CLASS ACTION ALLEGATIONS

18. This action is being commenced as a proposed class action, pursuant to Fed. R. Civ. P. 23.

19. The proposed class consists of all persons who received robocalls via the defendants' telecommunications services within the four years preceding the filing of this complaint.

20. This proposed class is so numerous that joinder of all members is impracticable.

21. There are questions of law or fact common to the class which predominate over any questions affecting only individual class members.

22. The claims of the representative plaintiff are typical of the claims of the class as a whole.

23. The representative plaintiff will fairly and adequately protect the interests of the class.

24. A class action is superior to other available methods of the fair and efficient adjudication of the controversy.

THE UNDERLYING FACTS

Overview of Robocalling Fraud Schemes

A. Robocalling Fraud Targeting Individuals in the United States

25. Upon information and belief, the robocalling fraud schemes in which the Defendants are engaged share the same characteristics. Individuals at call centers located abroad, many of which are operating out of India, are bombarding the U.S. telephone system every day with millions of robocalls intended to defraud individuals in the United States. Many of these

fraudsters impersonate U.S. government officials, foreign government officials, or well-known American businesses, in order to threaten, defraud, and extort money from robocall recipients. Robocalling technology, which allows fraudsters to send millions of calls per day all transmitting the same pre-recorded, fraudulent message, enables fraudsters to cast a wide net for elderly and vulnerable victims who are particularly susceptible to the threatening messages the fraudsters are sending. Even if only a small percentage of the recipients of a fraudulent call center's robocalls connect with potential victims, the fraudsters can still reap huge profits from their schemes.

26. Upon information and belief, foreign fraudsters operate many different schemes targeting individuals in the United States, but the Defendants' robocall schemes include the following categories of impersonation scams:

a. Social Security Administration ("SSA") Imposters: Defendants transmit recorded messages in which SSA imposters falsely claim that the call recipient's social security number has been used in criminal activity, the individual's Social Security benefits will be suspended, the individual has failed to appear before a grand jury and face imminent arrest, or the individual's social security number will be terminated. When a call recipient calls back or connects to the fraudster, the fraudster claims to be an SSA employee and typically tells the individual to transfer substantial funds to the SSA for safekeeping until a new social security number can be issued, at which point the individual's funds purportedly will be returned.

b. Internal Revenue Service ("IRS") and Treasury Imposters: Defendants transmit recorded messages in which IRS imposters falsely claim that the call recipient has been implicated in tax fraud, the individual has avoided attempts to enforce

criminal laws, the individual has avoided court appearances, or the individual faces imminent arrest. When a recipient calls back or connects to the fraudster, the fraudster claims to be an IRS or Treasury employee and typically tells the recipient to transfer funds to the IRS to resolve various fictitious tax and legal liabilities, or for safekeeping in order to avoid seizure of assets.

c. United States Citizenship and Immigration Services ("USCIS") Imposters: Defendants transmit recorded messages in which USCIS imposters falsely claim that the call recipient has failed to fill out immigration forms correctly, the individual faces imminent arrest or deportation, that the individual's home country has taken formal action that may result in deportation, or the individual has transferred money in a way that will result in deportation. When a call recipient calls back or connects to the fraudster, the fraudster claims to be a USCIS employee and typically tells the individual to pay various fees or fines to avoid immigration consequences.

d. Foreign Government Imposters: Defendants transmit recorded messages in which foreign government imposters, often in foreign languages, falsely claim to be from the U.S.-based consulate of a foreign government and that the call recipient faces problems with immigration status or a passport. When a call recipient calls back or connects to the fraudster, the fraudster falsely claims that the individual must pay various fees or fines in order to avoid immigration consequences such as deportation.

e. Tech Support Imposters: Defendants transmit recorded messages in which fraudsters operating tech support scams impersonate various well-known tech

companies such as Apple or Microsoft, and falsely claim that the call recipient has computer security problems that require assistance. When an individual connects with the fraudster, the fraudster instructs the individual to pay for fictitious tech support and computer security services, and to allow the fraudster remote access to the victim's bank accounts.

27. Upon information and belief, these robocalls are often "spoofed" so that they falsely appear on a victim's caller ID to originate from U.S. federal government agency phone numbers, such as the SSA's main customer service number, from local police departments, 911, or from the actual customer service phone numbers of legitimate U.S. businesses. These "spoofed" numbers are used to disguise the origin of the robocalls and the callers' identities, and to cloak them with the authority of government agencies or large businesses to induce potential victims to answer or return the calls. In reality, the calls originate from fraudsters operating abroad, and have no connection to any U.S. government agency or other legitimate enterprise.

28. Upon information and belief, individuals who answer or otherwise respond to these calls eventually speak to live fraudsters who tell the individuals lies intended to frighten and confuse them so that the fraudsters may begin to control their behavior and isolate them from authorities, friends, and family members. These lies often include that the individual's social security number or other personal information has been implicated in criminal activity, that the individual faces imminent arrest or deportation, and that the individual's assets are about to be forfeited to the government. Once an individual is overcome by fear and panic, the fraudsters keep them on the phone and offer reassurances that the individual's purported legal problems can be resolved through payment of money, or that the individual's money must be transferred for safekeeping to the government agency the fraudsters are impersonating. The fraudsters often

claim that the victim's payment will be returned to them in the immediate future. In reality, once the fraudsters are convinced they have extorted as much money as possible from the victim, they drop all contact, leaving the victim without meaningful recourse. Fraudsters receive victims' money through retail gift cards, bank wires, cash payments, cryptocurrency transfers, and other methods.

29. Upon information and belief, since October 2018, the most prolific robocalling scam impersonating U.S. government officials-and one engaged in by Defendants-is impersonation of the SSA. For example, a robocall sent to millions of phones in the United States in early 2019 contained the following message:

> Hello this call is from Department of Social Security Administration the reason you have received this phone call from our department is to inform you that there is a legal enforcement actions filed on your social security number for fraudulent activities so when you get this message kindly call back at the earliest possible on our number before we begin with the legal proceedings that is 619-[XXX]-[X:XXX] I repeat 619-[:XXX]-[X:XXX] thank you.

30. Upon information and belief, SSA received more than 465,000 complaints about fraudulent telephone impersonation of the Administration from October 1, 2018 through September 30, 2019. Losses associated with these complaints exceed $14 million. Similarly, the Federal Trade Commission ("FTC") reported that for 2018, its Consumer Sentinel database received more than 39,000 fraud complaints about SSA imposter calls, with estimated losses of approximately $11.5 million; for 2019, the FTC reported that SSA imposter call complaints rose to approximately 166,000 with associated losses of more than $37 million.[1] Complaint numbers

[1] Regarding government imposter fraud more broadly and not limited just to SSA imposters, the FTC's Consumer Sentinel database contains 255,223 complaints reflecting $128,479,054 in losses for 2018, and 389,563 complaints reflecting $152,946,623 in losses for 2019.

substantially underrepresent the extent of the problem, because most victims do not report their losses to the government.

B. How Calls From Foreign Fraudsters Reach U.S. Telephones

31. Upon information and belief, the Defendants' robocalling fraud schemes, which involve robocalls that originate abroad and target individuals in the United States, are all dependent on VoiP and related technology to create the calls. VoiP calls use a broadband internet connection-as opposed to an analog phone line-to place telephone calls locally, long distance, and internationally, without regard to whether the call recipient uses a cellular phone or a traditional, wired phone. The robocalling fraud schemes also require U.S.-based telecommunications companies-referred to as "gateway carriers" to introduce the foreign phone traffic into the U.S. phone system. A foreign call center or telecommunications company that places VoiP calls to U.S. telephones must have a relationship with a U.S. gateway carrier. From the gateway carrier, most VoiP calls will pass through a series ofU.S.-based VoiP carriers before reaching a consumer-facing "common carrier" such as AT&T or Verizon, and ultimately a potential victim's phone. One of the Defendants' roles in the fraudulent schemes is to serve as a gateway carrier for the fraudulent robocalls.

32. Upon information and belief, each provider in the chain that transmits a VoiP call maintains records, primarily for billing reasons, of all of the calls that pass through it. These records include the following information: the date and time of the call, the destination number (intended recipient), the source number from which the call was placed (sometimes a real number and sometimes a spoofed number), the name of the company that sent the call to the provider, and the downstream company to which the provider sent the call. These records are generated automatically as a call is routed through telecommunications infrastructure in a

manner that achieves the lowest cost to transmit a given call, known in the industry as "least-cost routing." Calls may be traced through these records back to their gateway carrier, and thus to their foreign source. The telecommunications industry refers to this tracing process as "traceback."

33. Upon information and belief, tracebacks of many different robocalling fraud schemes have led to the identification of Defendants as a gateway carrier willing to transmit huge volumes of fraudulent robocalls into the country, despite clear indicia of fraud in the call traffic and actual notice of fraud.

Defendants' Ongoing Participation in Robocalling Fraud Schemes

34. Upon information and belief, since at least 2016, the Defendants have knowingly provided U.S.-bound calling services to foreign fraudsters operating robocall scams, acting as a gateway carrier and passing robocalls into the U.S. telephone system by the millions. The Defendants are paid for each call they pass into and through the U.S. telephone system. In addition, the Defendants have provided return-calling services to the fraudsters operating the robocall scams, for which Defendants are also paid, enabling the fraudsters to establish contact with unwitting individuals after the individuals are deceived by a robocall.

35. Upon information and belief, there is substantial evidence of the Defendants' knowledge of the fraudulent nature of the calls they transmit, including call records showing high percentages of short-duration, unanswered calls passing through their systems by the millions; thousands of spoofed calls purporting to be from "911" and similar numbers originating from overseas; dozens of complaints, warnings, and inquiries from vendors and other telecommunications companies about fraud, spoofing, and short-duration "junk" calls; repeated warnings and inquiries from an industry trade group about the scam robocalls passing through

the Defendants' system; and receipt of numerous complaints from common-carrier telecommunications companies whose customers were victims of these fraud schemes.

A. Defendants Knowingly Introduce Fraudulent Robocalls into the U.S. Telephone System

36. Upon information and belief, in the telecommunications industry, high volumes of short-duration and unanswered calls are indicative of robocalls that are unwanted by the recipients, often because they are fraudulent. Defendants regularly transmit massive volumes of such calls. For example, a Government investigation has revealed a sample of more than 7.7 million calls that Defendant Global Voicecom routed through a single downstream VoiP carrier over 19 days in May and June 2019, months after Kaen's response to the FCC. Of those calls, approximately 86%, more than 6.6 million calls, were one second or less in duration, indicating exceedingly high levels of junk and fraudulent robocalls. Moreover, a small sample of approximately 330,000 of these calls was examined in greater detail; of these approximately 330,000 calls in that 19-day period, more than 270,000 (approximately 81%) were from source numbers (the numbers appearing on the recipients' caller IDs) identified as fraudulent robocalls. Similarly, of the more than 106,000 robocalls spoofing the SSA's toll-free customer service number in January and February 2019 that Defendant Global Voicecom transmitted into the United States, nearly 60% had a call duration of less than one second, and another 38% were between one and 60 seconds in duration. During that same period in January and February 2019, Defendant Global Voicecom also ran through its systems thousands of calls spoofing 911, 1911, and 11911, with similar short call durations.

37. Upon information and belief, Defendants provide inbound VoiP calling to the United States telecommunication system (referred to in the industry as "U.S. call termination") to customers located both here in the United States and abroad. Defendants provide unrestricted

VoiP calling, meaning they do not monitor or restrict the inbound calls a customer can place for either volume of calls or call duration. Defendants are paid for each call they pass into and through the U.S. phone system.

38. Upon information and belief, Defendants specifically market their services to foreign call centers and foreign VoiP carriers looking to transmit high volumes of robocalls to individuals in the United States. The TollFreeDeals website states "TollFreeDeals.com is your premier connection for call center and dialer termination. We are always looking for the best call center routes in the telecom industry. We specialize in short call duration traffic or call center traffic. We understand there is a need for it and we want to help you find all the channels you need!"

39. Upon information and belief, the FAQs on the TollFreeDeals website state, "Do you handle CC (Call Center)/Dialer Traffic? Yes- unlike many carriers we will handle your dialer and call center VoiP termination minutes. If you are looking for USA Dialer, Canada Dialer, or Australia Dialer please fill out our online interop form to test our routes."

40. Upon information and belief, Defendants regularly transmit massive volumes of short duration calls. For example, over 23 days in May and June of 2019, TollFreeDeals transmitted more than 720 million calls. Of those calls, more than 425 million, or 59% of the total calls, lasted less than one second in duration. In the telecommunications industry, high volumes of short-duration and unanswered calls are indicative of robocalls that are unwanted by the recipients, often because they are fraudulent. More than 24 million of those calls were placed to phone numbers with area codes in the Eastern District of New York. As Defendants' phone records show the ultimate destination number of every VoiP call they transmit, Defendants know they transmit fraudulent calls to potential victims in the Eastern District of New York.

41. Upon information and belief, during May and June of 2019, the Palumbos facilitated the delivery of more than 182 million calls through TollFreeDeals from a single India-based VoiP carrier co-conspirator to phones in the United States. One thousand different source numbers (the number from which a call is placed, and that shows up on the recipient's caller ID) accounted for more than 90% of those calls. According to data obtained from a robocall blocking company about calls identified as fraudulent robocalls in 2019, 79% of those 1000 source numbers have been identified as sending fraudulent robocalls. Consequently, TollFreeDeals transmitted an estimated 143 million fraudulent robocalls on behalf of that single India-based co-conspirator during May and June of 2019. Of those calls, an estimated 20% were Social Security imposter calls, 35% were loan approval scams, and 14% were Microsoft refund scams. The remaining calls were a mixture of IRS imposter, U.S. Treasury imposter, miscellaneous tech support imposter and other schemes.

42. Upon information and belief, Defendants' knowledge of the fraudulent nature of the telephone calls they deliver to potential victims on behalf of their co-conspirators is also evidenced by the numerous complaints, inquiries, and warnings regarding fraudulent robocalls that Defendants received from other telecommunications carriers and a telecommunications industry trade association since at least 2017. Despite receiving these complaints, inquiries, and warnings, Defendants nevertheless continued to transmit massive volumes of fraudulent robocalls from their co-conspirators to potential victims in the United States.

43. Upon information and belief, for example, in May 2017, AT&T notified Nicholas Palumbo that it had traced back to TollFreeDeals robocalls received by its customers that spoofed phone numbers belonging to USCIS and the Office of the Inspector General of the U.S. Department of Homeland Security ("DHS-OIG"). AT&T informed Nicholas Palumbo that the

callers who spoke to AT&T's customers impersonated U.S. Immigration Officers, and that AT&T had confirmed with USCIS and DHS-OIG that those agencies did not use any of the phone numbers at issue as a legitimate outbound caller ID. Nicholas Palumbo responded that the calls were transmitted to TollFreeDeals from an India-based VoiP carrier, and that he had blocked those two specific phone numbers. Blocking specific numbers is an ineffective means to stop fraudsters who are willing and have the ability to spoof any number as the caller ID number for their fraud calls.

44. Upon information and belief, in February 2019, AT&T notified Nicholas Palumbo that it had traced back 19 separate calls to AT&T customers that spoofed a US CIS phone number in order to "extort money from our customers." In Nicholas Palumbo's response to AT&T, he acknowledged that those calls were transmitted to TollFreeDeals from the same India-based VoiP carrier that had transmitted spoofed US CIS calls in 2017. Despite repeated warnings from AT&T that this foreign VoiP carrier was transmitting fraudulent government-impersonation robocalls, the Palumbos continued transmitting VoiP calls on behalf of this customer through at least as recently as June 2019.

45. Upon information and belief, the Palumbos have also received numerous warnings from telecommunications industry trade association US Telecom that both TollFreeDeals.com and SIP Retail have transmitted fraudulent robocalls, including government impersonation robocalls.

46. Upon information and belief, from May 2019 through January 2020, TollFreeDeals received 144 notifications from USTelecom that a fraudulent robocall had been traced back to TollFreeDeals. Of these notifications, 83 referenced SSA imposter fraud calls, 24 referenced Tech Support imposter fraud calls, ten referenced IRS imposter fraud calls, and one

referenced US CIS impersonation fraud calls. Each of these emails were sent to Nicholas Palumbo at his @tollfreedeals.com email address. Each email stated that a suspicious call had been traced back to TollFreeDeals's network and provided the call date, time and the source and destination phone numbers, to allow TollFreeDeals to identify the specific call at issue in its call logs (referred to in the industry as "call detail records"). Each email also provided a link to USTelecom's web-based traceback portal, where further information was provided about the specific fraudulent call at issue, included a recording of the fraudulent voicemail message that was sent to the recipient's phone.

47. Upon information and belief, in every case, either the email itself or the traceback pmial included a short description of the type of fraud at issue and the details of the fraudulent robocall campaign, such as:

> Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated voice claims suspicious activity on your social security number; press 1. Calls are from apparently random 8XX numbers or other geographic numbers. Call volume estimated at over a million transmitted spoofed US CIS calls in 2017.

48. Upon information and belief, despite repeated warnings from AT&T that this foreign VoiP canier was transmitting fraudulent government-impersonation robocalls, the Palumbos continued transmitting VoiP calls on behalf of this customer through at least as recently as June 2019.

49. Upon information and belief, the Palumbos have also received numerous warnings from telecommunications industry trade association US Telecom that both TollFreeDeals.com and SIP Retail have transmitted fraudulent robocalls, including government impersonation robocalls.

50. Upon information and belief, from May 2019 tluough January 2020, TollFreeDeals received 144 notifications from USTelecom that a fraudulent robocall had been traced back to TollFreeDeals. Of these notifications, 83 referenced SSA imposter fraud calls, 24 referenced Tech support imposter fraud calls, ten referenced IRS imposter fraud calls, and one referenced US CIS impersonation fraud calls. Each of these emails were sent to Nicholas Palumbo at his @tollfreedeals.com email address. Each email stated that a suspicious call had been traced back to TollFreeDeals's network and provided the call date, time and the source and destination phone numbers, to allow TollFreeDeals to identify the specific call at issue in its call logs (referred to in the industry as "call detail records"). Each email also provided a link to USTelecom's web-based traceback portal, where further information was provided about the specific fraudulent call at issue, included a recording of the fraudulent voicemail message that was sent to the recipient's phone.

51. Upon information and belief, in every case, either the email itself or the traceback portal included a short description of the type of fraud at issue and the details of the fraudulent robocall campaign.

52. Upon information and belief, since 2017, significant numbers of fraudulent robocalls have been traced back to the Defendants and brought to their attention. For example, U.S. common carrier AT&T has notified Defendants on numerous occasions about fraud traced back to Defendants' operations. These notices include a November 16, 2017, email to IP Dish:

> The following calls to AT&T cell phone customers were received using the spoofed caller ID numbers of a non-working number at the US Department of Homeland Security headquarters. Callers impersonated US Citizenship and Immigration[ ] Services personnel and defrauded an AT&T customer of $1,450.... Pursuant to the customer and carrier network fraud protection provisions of the

> Telecommunication Act and the Telephone Records Privacy Protection Act (47 USC 222(d)(2)), could you provide the name(s) of your upstream carriers? We are tracing these calls to their source so they can be stopped.

53. Upon information and belief, AT&T sent similar emails about USCIS impersonation scams to Defendants Kaen and Global Voicecom in September 2017, November 2017, April 2018, and July 2018. Similarly, AT&T emailed Defendants about SSA and other imposter robocalls on January 29, 2019:

> We have been receiving AT&T customers complaints about spoofing fraud from your network. In the first complaint calls are originating from a toll free number owned by the US Social Security Administration. Callers falsely claim to be US Government officials and attempt to extort money from our customers. We have verified this number is not out-pulsed as a legitimate caller ID by the real US Social Security Administration....
>
> In the second complaint calls are originating from the toll free number of DirecTV (AT&T). Callers falsely claim to be AT&T/DirecTV technical reps and social engineer remote access to our customer's computers in order to make fraudulent wire transfers from online banking applications....
>
> Could you provide the names and contact numbers of the parties that sent these calls to your network.

54. Upon information and belief, AT&T sent similar warning notices about SSA imposter calls to Defendants Kaen and Global Voicecom in February 2019 and May 2019.

55. Upon information and belief, another VoiP carrier that received call traffic from Defendants, Peerless Network, Inc., sent even more warning notices and inquiries to Defendants. For example, Peerless Network sent a warning notice about spoofed calls in September 2018 with a request that Defendants investigate and "take the appropriate action." Peerless Network sent approximately 12 of these warning notices between September 2018 and March 2019.

56. Upon information and belief, not only have other telecommunications companies provided warnings and notices to Defendants as a result of tracebacks, but a leading industry

trade group, USTelecom, has done the same. For example, USTelecom traced back an August 19, 2019 robocall that originated from India and came through Defendant Global Voicecom as the gateway carrier. The robocall was also routed through Defendant KAT Telecom. This robocall stated that there was "suspicious activity" associated with the individual's social security number. USTelecom provided the following warning notice in its correspondence to Defendant Global Voicecom on August 27, 2019:

> Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated voice claims suspicious activity on your social security number; press 1. Calls are from apparently random 8XX numbers or other geographic numbers. Call volume estimated at over a million per day. Because Caller-ID changes with each call, blocking the ANI 8 is not effective.

57. Upon information and belief, blocking specific telephone numbers is an ineffective means to stop fraudsters who are willing- and have the ready ability-to spoof any number as the caller ID number for their fraudulent robocalls. For example, in January and February 2019, Defendants transmitted fraudulent robocalls spoofing 911, 1911, and 11911. Nevertheless, if the Defendants responded at all to these notices and warnings from other telecommunications-industry actors, they routinely responded that the "offending" number had been blocked, as though the spoofed telephone number and not the caller were responsible for the fraud.

58. Upon information and belief, similarly, USTelecom traced an October 3, 2019 robocall to Defendant Global Voicecom as the gateway carrier. This robocall also originated from India. USTelecom provided the following warning notice in its October 11, 2019 correspondence to Defendant Global Voicecom:

> Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Calls placed from specific numbers obtained by scammers, using an automated

> voice to inform called party that they are in trouble with IRS and will be arrested. Called party is instructed to call back to speak to an agent. .. We are using traceback to try to find the source(s) of the millions of outbound calls that are being made to initiate the scam.

59. Upon information and belief, USTelecom's records indicate that this robocall was transcribed in part as follows:

> This call is from Federal Tax and audit division of internal revenue services. This message is intended to contact you regarding an enforcement action executed by the US treasury intending your serious attention. Ignoring this will be an intentional second attempt to avoid initial appearance before a magistrate judge or a grand jury for federal criminal offense. This is a final attempt to reach you to resolve this issue immediately and to speak to a federal agent to call us back on 510-[XXX]-[XXXX]. I repeat 510-[XXX]-[XXXX].

60. Upon information and belief, USTelecom identified Defendants as the gateway carrier for foreign fraudulent robocalls on at least eighteen other occasions in the latter half of 2019 alone, each time providing similar warning notices about the nature of the scam robocalls. USTelecom's records indicate that on nearly all of these 2019 tracebacks, the scam robocalls came from the same company in India.

61. Upon information and belief, Defendants transmitted another group of fraudulent robocalls that· spoofed the phone number for a foreign government consulate in New York, New York. These calls conveyed foreign-language messages about problems with the individual's immigration status or passport. Like with SSA imposter robocalls and other U.S. government-imposter scams, individuals who returned the calls to the consulate imposters were told lies intended to frighten them and make them think there are imminent consequences for involvement in criminal activity, and that funds must be transferred to the fraudsters to resolve the matters. Like with the SSA imposter scams, once the fraudsters are convinced they have extorted as much money as possible, they drop all contact with the victim. In 2018, the FCC

traced this consulate imposter scam back to Kaen and IP Dish, who informed the FCC that the calls came from a Hong Kong entity that was making tens of thousands of calls per day. The FTC's Consumer Sentinel database reflects more than 1,000 complaints related to the spoofed phone number of the consulate. These complaints relate hundreds of thousands of dollars in victim losses. Defendants continue to conduct business with this Hong Kong entity more than a year later.

62. Upon information and belief, despite these notices and numerous others, Defendants continue to pass fraudulent robocalls into the U.S. telephone system to millions of U.S. telephones every day.

B. Defendants Provide Return-Calling and Toll-Free Services for Robocall Schemes

63. Upon information and belief, not only do Defendants knowingly pass fraudulent robocalls by the millions into the U.S. telephone system, but they also provide return-calling services to fraudsters so that potential victims can call them back. These toll-free and direct-inward-dial ("DID") telephone numbers and related services are provided in the robocall message as call-back numbers, and appear to be U.S. telephone numbers and thus enable fraudsters to further deceive individuals about the robocall's origin and the identities and locations of the fraudsters at the other end of the call. In reality, what appears to the individual to be a U.S. telephone number is actually a telephone number that Defendants register to an internet address designated by the foreign fraudsters. Thus, the DID and toll-free numbers can be used to ring telephones anywhere in the world.

64. Upon information and belief, while DID and toll-free numbers used for return-calling purposes cannot be "spoofed" like outgoing robocalls, the use of a U.S. DID or toll-free number in Defendants' robocalls schemes serves much the same purpose as spoofing-deception.

The DID and toll-free services provided by Defendants use VoiP technology to direct potential victims' return calls from the United States to the foreign fraudsters' call centers. The Defendants have knowingly provided hundreds of these DID and toll-free numbers and associated calling services to foreign robocall fraudsters.

1. DID Numbers Used to Further Robocalling Fraud Schemes

65. Upon information and belief, like telephone numbers used to make U.S.-bound robocalls, DID numbers can be traced to identify their providers and users. This process was used to identify DID numbers provided by the Defendants for use in the fraudulent robocall schemes. For example, records obtained from one U.S. company demonstrate that it assigned 902 DID telephone numbers to Defendant Global Voicecom. Approximately 55% of these DID telephone numbers are associated with more than 28,000 complaints in the FTC's Consumer Sentinel database. One of the 902 DID telephone numbers appeared in a robocall sent to millions of U.S. telephones in early 2019:

> Hello this call is from Department of Social Security Administration the reason you have received this phone call from our department is to inform you that there is a legal enforcement actions filed on your social security number for fraudulent activities so when you get this message kindly call back at the earliest possible on our number before we begin with the legal proceedings that is 619-[:XXX]-[XXXX] I repeat 619-[:XXX]-[:XXXX] thank you.

66. Upon information and belief, at the time of the robocalls, this DID telephone number was assigned to Defendant Global Voicecom, which used that DID telephone number to provide return-calling services to the overseas fraudsters. Individuals who return calls like these put themselves in a pool of likely victims, insofar as the individuals self-select through belief that the message was sufficiently credible to warrant a return call. Upon returning the call to 619-[:XXX]-[:XXXX], individuals were told that they were speaking to SSA agents, who offered to

resolve the purported problems that prompted the call by way of immediate payment of funds. In reality, the person speaking to the individual was a fraudster, unaffiliated with the U.S. government.

67. Upon information and belief, beginning as early as September 2017 and continuing through the present, the U.S. company that assigned these 902 DID numbers to Defendants provided numerous warning notices about how the numbers were being used to perpetrate fraud. For example, that company provided the following warning notice to Defendant Global Voicecom on September 13,2017 and included the substance of several complaints about fraud:

> The DID: 847[XXXXX:XX] which we show assigned to you, is being used for fraudulent purposes. The US Treasury Department has provided us with a few complaints which are listed below. Because of the nature of the complaints, we have disabled this number on our network.
>
> I received a call from 484-[:XXX]-[:XXXX] claiming that I was a subject of Treasury Fraud. [T]hey said to call back at 847-[:X:XX]-[:XXXX]. The call was received on Friday September 8th at 4 pm. I live in Philadelphia, in the EST zone. They claimed I would be sued if I did not call back.
>
> I received a voicemail message with an automated recording claiming to be from the US Dept. of Treasury regarding tax fraud in my name. The call back number was 847-[XXX]-[:XXXX]. No one answered the return call. I recently submitted via mail my 3rd installment of2017 taxes, so I hope nothing has gone wrong in the process of receiving my payment. Is this a known scam number? Thank you.

68. Upon information and belief, the voice message states (Pre-recorded): "Treasury my badge number is 4874. The nature and purpose of this call is regarding an enforcement action which has been executed by the [U.S.] treasury department regarding tax fraud against your name. Ignoring this would be an intentional attempt to avoid initial appearance before the majesty does or exempt or enforce criminal offence. Before this matter goes to federal claim, court house, or before you get arrested. Kindly call us back as soon as possible. The number to

reach us is 847-[X:XX]-[:XXXX], let me repeat the number 847-[X:XX]-[:XXXX]. Hope to hear from you soon before the charges are pressed against you. Thank you."

69. Upon information and belief, through the course of the ensuing years, Defendants continued to receive numerous similar warning notices about DID numbers and related services they provide. Defendants effectively ignored the warnings and never terminated the fraudsters' access to DID numbers for return calls.

70. Upon information and belief, in the course of a Government investigation, SSA OIG agents obtained from Global Voicecom call records for seven of the 902 DID numbers assigned to Defendant Global Voicecom that are associated with SSA imposter robocalls. According to Defendants' own records, Defendants provided these seven DID numbers to the same Indian entity that Defendant Global Voicecom identified to USTelecom as the gateway carrier for numerous government imposter scam robocalls.

71. Upon information and belief, these DID call records reveal that more than 10 million calls were placed in 2019 from more than 4.5 million unique phone numbers to the 902 DID numbers assigned to Defendant Global Voicecom. More than 240,000 of these calls were from area codes for the Eastern District of NewYork.

2. Toll-Free Numbers Used to Further Robocalling Fraud Schemes

72. Upon information and belief, records from the FTC demonstrate that Defendants Global Voicecom and Jon Kaen are associated with more than 1000 October 2019 SSA-imposter robocalls to the FTC's offices. These robocalls appeared to originate from a toll-free telephone number. Toll-free numbers work in a manner similar to DID numbers, but are structured differently by the FCC and telecommunications industry. Somos, Inc. is the FCC-designated national administrator of the U.S. toll-free calling system. Among other functions within the

industry, Somos registers "responsible organizations" that are authorized to provide toll-free numbers to their customers and to register those numbers in the national registry that the industry uses to direct toll-free telephone traffic. On October 23 and 24, 2019, the FTC's offices received approximately 1,000 robocalls with the following recording:

> ...social security on an immediate basis as your social has been found some suspicious for committing fraudulent activities across the United State. Before we go ahead and suspend your social security permanently, we want you to call us back on our department toll free number at 877-[XXX]-[XXXX]. I repeat 8-877-[:XXX]- [XXXX]. Do not disregard this message, and call us back as soon as possible. Thank you.

73. Upon information and belief, the toll-free 877 number appeared on the FTC's caller ID as well as in the actual robocall message as the return-call number. On October 24, 2019, an FTC investigator contacted Somos to determine which responsible organization was associated with that toll-free number, which Somos duly provided. The FTC investigator then contacted that responsible organization, who informed the investigator that the number was assigned to Defendants Global Voicecom and Jon Kaen.

74. Upon information and belief, that responsible organization provided numerous notices to Defendants concerning the toll-free numbers assigned to Global Voicecom and how they were being used to facilitate robocalling fraud, doing so 37 times between March 2019 and October 2019. For example, on April 8, 2019, the responsible organization emailed Defendant Global Voicecom: "We received a scam complaint on the number 888-[:XXX]-[:XXXX] and were asked to disconnect it. We dialed this number and found it was someone impersonating Microsoft, and is still connected." Similarly, on June 11, 2019, the responsible organization emailed Defendant Global Voicecom: "Please know that we have rec[ei]ved a serious complaint on TFN 888-[:XXX]-[:XXXX], which we see i[s] assigned to your account. This number was

reported as a part of an "Amazon Customer Support Scam." On August 26, 2019, the responsible organization emailed Defendant Global Voicecom: "Please note that we have received reports that 877-[XxX]-[XXXX] is being used to spoof Bank of America. Can you please look into this, inform us of your results and take action if necessary?" To each of the dozens of notices, Defendants responded to the effect that the "offending" number has been blocked, as if the spoofed telephone number and not the caller were committing fraud, but never that they terminated the sources of the fraudulent robocalls.

75. The FTC's Consumer Sentinel reflects more than 1,400 complaints associated with the toll-free numbers assigned to Defendant Global Voicecom.

76. Upon information and belief, not only do Defendants knowingly pass fraudulent robocalls by the millions into the U.S. telephone system, but they also provide return-calling services to fraudsters so that potential victims can call them back. These toll-free telephone numbers and related services are provided in the robocall message as call-back numbers, and appear to be U.S. telephone numbers and thus enable fraudsters to further deceive individuals about the robocall's origin and the identities and locations of the fraudsters at the other end of the call. In reality, what appears to the individual to be a U.S. telephone number is just a telephone number that Defendants register to an internet address designated by the fraudsters. Thus, the toll-free numbers can be used to ring telephones anywhere in the world.

77. Upon information and belief, while toll-free numbers used for return-calling purposes cannot be "spoofed" like outgoing robocalls, the use of a U.S. toll-free number in Defendants' robocalls schemes serves much the same purpose as spoofing--deception. The toll-free services provided by Defendants use VoiP technology to direct potential victims' return calls from the United States to the foreign fraudsters' call centers. The Defendants have

knowingly provided toll-free numbers and associated calling services to foreign robocall fraudsters.

78. Upon information and belief, all toll-free numbers in the United States are administered by Somos, Inc., a company designated by the Federal Communications Commission ("FCC") as the national administrator of the U.S. toll-free calling system and its database. Among other functions within the industry, Somos registers "Responsible Organizations," that are authorized to provide toll free numbers to their customers and to register those numbers in the national registry that the industry uses to direct toll-free telephone traffic. Defendants obtain toll-free numbers on behalf of their customers from one or more Responsible Organizations.

79. Upon information and belief, on July 31, 2019, an employee of a Responsible Organization sent the message below to Nicholas Palumbo via his @tollfreedeals.com email address:

> Hello,
>
> We received a call yesterday (at 6 pm) that we didn't answer. Calling Number: +844[XXXXXXX] Requesting to call back: 844-[XX:X:]-[XXXX] Please see the attached audio and screenshot of the voicemail transcript. Shut down this user immediately as it was associated with the customer account of [TollFreeDeals customer]. These types of scam calls are prohibited from our network and further fi·audulent calls from the same customer account will result in termination of said customer account. The number of 844-[XX:X:]-[X:X:XX] has been removed from your account in order to protect the integrity of our network.

80. Upon information and belief, the attached audio file of a voicemail message stated:

> tomorrow $399.99 is going to be deducted from your account for the remainder of your computer services. If you want to cancel the subscription, please press 1 to talk to our cancellation officer. Or you can call us back on our help line number l-

> 844-[XX:X:]-[XX:X:X]. I'll repeat the help line number 1-844-[XX:X:]-[XXXX]. Thank you.

81. Upon information and belief, over the course of the next two weeks, employees of the Responsible Organization sent an additional six emails to Nicholas Palumbo, notifying him that the Responsible Organization was removing eight additional toll-free numbers from the accounts of two TollFreeDeals customers, because those numbers had been shown to be used in Tech Support impersonation scams and scams impersonating Amazon customer service. In response to each email, Nicholas Palumbo responded simply that he had let the customer of TollFreeDeals know.

82. Upon information and belief, on August 12,2019, an employee of the Responsible Organization emailed Nicholas Palumbo and stated:

> Good afternoon Nick,
>
> I wanted to reach out to inform you that we have disabled the account of [TollFreeDeals customer] due to fraudulent complaints. Unfmiunately, we do get a lot of complaints about customers under your reseller account. Our first line of defense when issues like arise we deactivate the customer's account. I am informing you that if we do receive any additional complaints about any of your other customers under your re-seller account, we will be forced to deactivate your account.

83. Upon information and belief, Nicholas Palumbo responded "I let him know," then responded further, "I will be porting clients over[.] Can't take that chance." In the telecommunications industry, to "port a number" means to move an existing phone number from one provider to another. In effect, Nicholas Palumbo was stating that he planned to take the toll-free numbers registered to his customers through the Responsible Organization who had warned him about fraudulent calls, and move those same numbers to another provider on behalf of his customers.

Harm to Victims

84. Upon information and belief, Defendants' fraudulent schemes have caused substantial harm to numerous victims, including many victims located in the Eastern District of New York. It is estimated that Defendants and their foreign co-conspirators defrauded victims out of millions of dollars per year through fraudulent robocalls and return-calling services. If allowed to continue, these losses will continue to rise and result in further harm to victims.

85. In addition to the massive cumulative effect of these fraud schemes on U.S. victims, the harm can be devastating to individual victims. Victims have faced terrifying threats from fraudsters impersonating government officials and have lost substantial sums of money.

86. Defendants'· fraudulent schemes are ongoing and wide-ranging. Absent injunctive relief by this Court, the Defendants will continue to cause injury to victims in this District and throughout the United States, and the victims' losses will continue to mount.

Government Action

87. The Government has filed two actions on these facts, *USA v. Palumbo, et al.*, EDNY case no. 20-cv-473, and *USA v. Kahen, et al.*, EDNY case no. 20-474.

AS AND FOR A FIRST CLAIM FOR RELIEF

88. Plaintiff repeats and re-alleges each of the foregoing allegations with the same force and effect as if more fully set forth herein.

89. The plaintiff, and each member of the proposed plaintiff class, has received numerous robocalls which, upon information and belief, were carried, processed, connected, placed, routed, and/or facilitated by the defendants and/or the agents, servants, employees, and related entities.

90. By their conduct, Defendants have violated the Telephone Consumer Protection Act ("TCPA"), 47 U.S.C. § 227.

91. The depth and breadth of Defendants' violation of the TCPA is astonishing, as it continued for years, involved hundreds of millions of calls, and continued despite multiple complaints, inquiries, and warnings, and thus could only have been deliberate conduct.

92. Defendants disregarded all laws and regulations, ignored do-not-call lists, and acted with complete lawlessness.

93. Pursuant to the TCPA, Plaintiff, and each member of the plaintiff class, may recover the greater of actual damages or $500, and the Court may, in its discretion, increase the amount of the award up to three times that amount.

94. The defendants are jointly and severally liable.

95. By reason of the foregoing, Plaintiff, and each member of the plaintiff class, is entitled to recover the full extent of his damages, in an amount to be determined by the jury at trial.

JURY TRIAL DEMANDED

96. Plaintiff demands a trial by jury of all issues triable to a jury.

WHEREFORE, the plaintiff demands judgment against the defendants in the amounts and for the relief requested herein, plus attorney's fees to the extent permitted by law.

Dated: Brooklyn, New York
January 29, 2020

Yours,

THE BERKMAN LAW OFFICE, LLC
Attorneys for the plaintiff

by: _____
Robert J. Tolchin

111 Livingston Street, Suite 1928
Brooklyn, New York 11201
(718) 855-3627

EXHIBIT 2

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

Plaintiff,

v.

NICHOLAS PALUMBO, NATASHA PALUMBO, ECOMMERCE NATIONAL, LLC d/b/a Tollfreedeals.com, and SIP RETAIL d/b/a sipretail.com,

Defendants.

COMPLAINT

Civil Action No.

CV20-473

KORMAN, J.

MANN. M.J.

Plaintiff, the UNITED STATES OF AMERICA, by and through the undersigned attorneys, hereby alleges as follows:

INTRODUCTION

1. The United States brings this action for a temporary restraining order, preliminary and permanent injunctions, and other equitable relief pursuant to 18 U.S.C. § 1345, in order to enjoin the ongoing commission of criminal wire fraud in violation of 18 U.S.C. § 1343 and conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349. The United States seeks to prevent continuing and substantial injury to the victims of fraud.

2. Since at least 2016 and continuing through the present, Defendants, together with one or more co-conspirators, have used the U.S. telephone system to engage in predatory wire fraud schemes that victimize individuals throughout the United States, including individuals within the Eastern District of New York and significant numbers of elderly and vulnerable victims.

Defendants are VoIP[1] carriers, and their principals, that serve as "gateway carriers,"[2] facilitating the delivery of millions of fraudulent "robocalls"[3] every day from foreign call centers and foreign VoIP carriers to the U.S. telecommunications system and ultimately to phones throughout the United States. The Defendants thus provide foreign fraudsters the means to access the U.S. telephone system, knowingly passing millions of fraudulent robocalls intended to deceive the recipient into: (1) answering or returning the call, and (2) paying money to the perpetrators of the schemes.

3. Through these robocalls, fraudsters operating overseas impersonate government entities and well-known businesses by "spoofing"[4] legitimate phone numbers and sending recorded messages that are transmitted across the internet to telephones throughout the United States. These robocalls purport to be from federal government agencies, elements of foreign governments, and legitimate businesses, conveying alarming messages, such as that the call recipient's social security number or other personal information has been compromised or otherwise connected to criminal activity; the recipient faces imminent arrest; the recipient's assets are being frozen; the recipient's bank and credit accounts have suspect activity; the recipient's benefits are being stopped; the recipient faces imminent deportation; or combinations

---

[1] VoIP stands for voice-over-internet protocol and allows users to place phone calls over a broadband internet connection.

[2] As set forth in greater detail herein, "gateway carriers" are the first in a chain of VoIP carriers located in the United States that facilitate the delivery of foreign VoIP calls to recipients in the United States.

[3] "Robocall" means a call made through an automated process that places large volumes of telephone calls over the internet in order to deliver recorded messages, in contrast to calls placed one at a time by a live person.

[4] The practice of making a false number appear on the recipient's caller ID is known as "spoofing."

of these things—all lies intended to induce potential victims to speak to the fraudsters. When individuals answer the calls or return voicemail messages, the fraudsters offer to "resolve" these legal matters by immediate transfers of funds to settle the purported legal obligation, or to hold the individual's assets only temporarily while the crisis resolves. In reality, the individual is neither under investigation nor in legal jeopardy, and the same threatening robocall was made simultaneously to thousands of other U.S. telephones.

4. Not only do Defendants deliver vast numbers of fraudulent robocalls every day, but they also participate in the fraudulent schemes by providing return-calling services the fraudsters use to establish contact with potential victims. Robocall messages will often provide domestic and toll-free call-back numbers; potential victims who call these numbers connect to the overseas fraudsters, who then try to extort and defraud the potential victims.

5. Defendants profit from these fraudulent robocall schemes by receiving payment from their co-conspirators for the services Defendants provide. Often, these payments consist of victim proceeds, a portion of which is deposited directly into Defendants' accounts in the United States, before the remainder is transmitted to the fraudsters overseas.

6. Since at least 2016 and continuing through the present, as a result of their conduct, Defendants and their co-conspirators have defrauded numerous victims out of millions of dollars, including victims in the Eastern District of New York.

7. For the reasons stated herein, the United States requests injunctive relief pursuant to 18 U.S.C. § 1345 to enjoin Defendants' ongoing schemes to commit wire fraud in violation of 18 U.S.C. § 1343 and conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349.[5]

[5] This case is one of two cases being filed simultaneously in which the United States Department of Justice, for the first time, seeks to enjoin telecommunications companies from participating in robocalling fraud schemes pursuant to 18 U.S.C. § 1345.

JURISDICTION AND VENUE

8. The Court has subject matter jurisdiction over this action pursuant to 18 U.S.C. § 1345 and 28 U.S.C. §§ 1331 and 1345.

9. Venue lies in this district pursuant to 28 U.S.C. § 1391(b)(2).

PARTIES

10. Plaintiff is the United States of America.

11. Defendants Nicholas and Natasha Palumbo own and control Ecommerce National, LLC, doing business as TollFreeDeals.com and SIP Retail, LLC, also doing business as SipRetail.com (the "Corporate Defendants"), which the Palumbos utilize in furtherance of the fraudulent robocall schemes. The Palumbos operate the Corporate Defendants from their home in Paradise Valley, Arizona, and on information and belief, the Palumbos operate SIP Retail as an alter ego of Ecommerce. From their home in Paradise Valley, Arizona, the Palumbos operate the Corporate Defendants as fraudulent enterprises.

12. Defendant Ecommerce is a corporation organized and existing under the laws of the State of Arizona. Ecommerce does business as TollFreeDeals.com, and will be referred to throughout this Complaint as TollFreeDeals. TollFreeDeals' principal place of business is located at the Palumbos' home in Paradise Valley, Arizona. Nicholas Palumbo is the Chief Executive Officer of TollFreeDeals and Natasha Palumbo is the Vice President of Business Development.

13. Defendant SIP Retail, LLC, also doing business as SipRetail.com ("SIP Retail"), is a corporation organized and existing under the laws of the State of Arizona. SIP Retail's principal place of business is located at the Palumbos' home in Paradise Valley, Arizona. Natasha Palumbo is the Chief Executive Officer of SIP Retail. SIP Retail provides VoIP carrier services for some of the same customers as TollFreeDeals, including foreign VoIP carriers that

transmit millions of calls every week destined for the phones of residents of the Eastern District of New York.

OVERVIEW OF THE ROBOCALLING FRAUD SCHEMES

A. Robocalling Fraud Targeting Individual in the United States

14. The robocalling fraud schemes in which the Defendants are engaged share the same characteristics. Individuals at call centers located abroad, many of which are operating out of India, are bombarding the U.S. telephone system daily with millions of robocalls intended to defraud individuals in the United States. Many of these fraudsters impersonate U.S. government officials, foreign government officials, or well-known American businesses, in order to threaten, defraud, and extort money from robocall recipients. Robocalling technology, which allows fraudsters to send millions of calls per day all transmitting the same pre-recorded, fraudulent message, enables fraudsters to cast a wide net for elderly and vulnerable victims who are particularly susceptible to the threatening messages the fraudsters are sending. Even if only a small percentage of the recipients of a fraudulent call center's robocalls connect with potential victims, the fraudsters can still reap huge profits from their schemes.

15. Foreign fraudsters operate many different scams targeting individuals in the United States, but the Defendants' robocall schemes include the following categories of impersonation scams:

a. *Social Security Administration ("SSA") Imposters*: Defendants transmit recorded messages in which SSA imposters falsely claim that the call recipient's social security number has been used in criminal activity, the recipient's Social Security benefits will be suspended, the recipient has failed to appear before a grand jury and faces imminent arrest, or the recipient's social security number will be

terminated. When a recipient calls back or connects to the fraudster, the fraudster claims to be an SSA employee and typically tells the individual to transfer substantial funds to the SSA for safekeeping until a new social security number can be issued, at which point the funds purportedly will be returned.

b. *Internal Revenue Service ("IRS") Imposters*: Defendants transmit recorded messages in which IRS imposters falsely claim that the call recipient has been implicated in tax fraud, has avoided attempts to enforce criminal laws, has avoided court appearances, or the recipient faces imminent arrest. When a recipient calls back or connects to the fraudster, the fraudster claims to be an IRS or Treasury employee and typically directs the recipient to transfer funds to the IRS to resolve various fictitious tax and legal liabilities, or for safekeeping in order to avoid seizure of assets.

c. *United States Citizenship and Immigration Services ("USCIS") Imposters*: Defendants transmit recorded messages in which USCIS imposters falsely claim that the recipient has failed to fill out immigration forms correctly, the recipient faces imminent arrest or deportation, the recipient's home country has taken formal action against the recipient that may result in deportation, or the recipient has transferred money in a way that will result in deportation. When a recipient calls back or connects to the fraudster, the fraudster claims to be a USCIS employee and typically tells the recipient to pay various fees or fines to avoid immigration consequences.

d. *Tech Support Imposters*: Defendants transmit recorded messages in which fraudsters operating tech support scams impersonate various well-known tech

companies such as Apple or Microsoft, and falsely claim that the recipient has computer security problems that require assistance. When an individual connects with the fraudster, the fraudster instructs the individual to pay for fictitious tech support and computer security services, and to allow the fraudster remote access to the victim's bank accounts.

e. *Loan Approval Scams*: Defendants transmit recorded messages in which fraudsters operating loan approval scams impersonate a "lender" offering a great, guaranteed rate on a "pre-approved" loan. When a customer connects with the fraudster, the fraudster will emphasize that a poor credit history does not matter, and all the call recipient has to do to secure the pre-approved loan is pay a one-time fee up front.

16. These robocalls are often "spoofed" so that they falsely appear on a victim's caller ID to originate from U.S. federal government agency phone numbers, such as the SSA's main customer service number, local police departments, 911, or the actual customer service phone numbers of legitimate U.S. businesses. These "spoofed" numbers are used to disguise the origin of the robocalls and the caller's identities, and to cloak them with the authority of government agencies or large businesses to induce potential victims to answer or return the calls. In reality, the calls originate from fraudsters operating abroad, and have no connection to any U.S. government agency or other legitimate enterprise.

17. Individuals who answer or return these calls eventually speak to live fraudsters who tell the individuals lies intended to frighten and confuse them so that the fraudsters may begin to control their behavior and isolate them from authorities, friends, and family members. These lies often include that the individual's social security number or other personal

information has been implicated in criminal activity, that the individual faces imminent arrest or deportation, and that the individual's assets are about to be forfeited to the government. Once an individual is overcome by fear and panic, the fraudsters keep them on the phone and offer reassurances that the individual's purported legal problems can be resolved through payment of money, or that the individual's money must be transferred to the government agency the fraudsters are impersonating. The fraudsters often claim that the victim's payment will be returned in the immediate future. In reality, once the fraudsters are convinced they have extorted as much money as possible from the victim, they drop all contact, leaving the victim without meaningful recourse. Fraudsters receive victims' money through retail gift cards, bank wires, cash payments, cryptocurrency transfers, and other methods.

18. Since October 2018, the most prolific robocalling scam impersonating U.S. government officials—and one engaged in by Defendants—is impersonation of the SSA. For example, a robocall sent to millions of phones in the United States in early 2019 contained the following message:

> Hello this call is from Department of Social Security Administration the reason you have received this phone call from our department is to inform you that there is a legal enforcement actions filed on your social security number for fraudulent activities so when you get this message kindly call back at the earliest possible on our number before we begin with the legal proceedings that is 619-XXX-XXXX I repeat 619-XXX-XXXX thank you.

19. SSA received more than 465,000 complaints about fraudulent telephone impersonation of the Administration from October 1, 2018 through September 30, 2019. Losses associated with these complaints exceed $14 million. Similarly, the Federal Trade Commission ("FTC") reported that during 2018, its Consumer Sentinel database received more than 39,000 fraud complaints about SSA imposters, with estimated victim losses of approximately $11.5 million; for 2019, the FTC reported that SSA imposter call complaints rose to approximately

166,000 with associated losses of more than $37 million.[6] Complaint numbers substantially underrepresent the extent of the problem, because most victims do not report their losses to the government.

B. How Calls From Foreign Fraudsters Reach U.S. Telephones

20. The Defendants' robocalling fraud schemes, which involve robocalls that originate abroad and target individuals in the United States, are all dependent on VoIP and related technology to create the calls. VoIP calls use a broadband Internet connection – as opposed to an analog phone line – to place telephone calls locally, long distance, and internationally, without regard to whether the call recipient uses a cellular phone or a traditional, wired phone. The robocalling fraud schemes also require U.S. based telecommunications companies – referred to as "gateway carriers" – to introduce the foreign phone traffic into the U.S. phone system. A foreign call center or telecommunications company that places VoIP calls to U.S. telephones must have a relationship with a U.S. gateway carrier. From the gateway carrier, most VoIP calls will pass through a series of U.S.-based VoIP carriers before reaching a consumer-facing "common carrier" such as AT&T or Verizon, and ultimately a potential victim's phone. One of the Defendants' roles in the fraudulent schemes is to serve as a gateway carrier for the fraudulent robocalls.

21. Each provider in the chain that transmits a VoIP call maintains records, primarily for billing reasons, of all of the calls that pass through it. These records include the following information: the date and time of the call, the destination number (intended recipient), the source

[6] Regarding government imposter fraud more broadly and not limited just to SSA imposters, the FTC's Consumer Sentinel database contains 255,223 complaints reflecting $128,479,054 in losses for 2018, and 389,563 complaints reflecting $152,946,623 in losses for 2019.

number from which the call was placed (sometimes a real number and sometimes a spoofed number), the name of the company that sent the call to the provider, and the downstream company to which the provider sent the call. These records are generated automatically as a call is routed through telecommunications infrastructure in a manner that achieves the lowest cost to transmit a given call, known in the industry as "least-cost routing." Calls may be traced through these records back to their gateway carrier, and thus to their foreign source. The telecommunications industry refers to this process as "traceback."

22. Tracebacks of many different robocalling fraud schemes have led to the identification of Defendants as a gateway carrier willing to transmit huge volumes of fraudulent robocalls into the country, despite clear indicia of fraud in the call traffic and actual notice of fraud.

DEFENDANTS' ONGOING PARTICIPATION IN ROBOCALLING FRAUD SCHEMES

23. Since at least 2016, and continuing through the present, Defendants have knowingly provided U.S.-bound calling services to foreign fraudsters operating robocall scams, acting as a gateway carrier and passing robocalls into the U.S. telephone system by the millions. The Defendants are paid for each call they pass into and through the U.S. phone system. In addition, the Defendants have provided return-calling services to the fraudsters operating the robocall scams, for which Defendants are also paid, enabling fraudsters to establish contact with unwitting individuals after the individuals are deceived by a robocall.

24. There is substantial evidence of the Defendants' knowledge of the fraudulent nature of the calls they transmit, including call records showing high percentages of short-

duration, unanswered calls[7] passing through their systems by the millions; thousands of spoofed calls originating from overseas, purporting to be from "911" and similar numbers; dozens of complaints and warnings from other telecommunications companies about fraud, spoofing, and short-duration "junk" calls; repeated warnings and inquiries from a telecommunications industry trade group about the fraudulent robocalls passing through the Defendants' system; and receipt of payment from their foreign customers in the form of large, suspicious cash deposits by various individuals throughout the United States directly into Defendants' bank accounts.

A. Defendants Knowingly Introduce Fraudulent Robocalls into the U.S. Telephone System

25. Defendants provide inbound VoIP calling to the United States telecommunication system (referred to in the industry as "U.S. call termination") to customers located both here in the United States and abroad. Defendants provide unrestricted VoIP calling, meaning they do not monitor or restrict the inbound calls a customer can place for either volume of calls or call duration. Defendants are paid for each call they pass into and through the U.S. phone system.

26. Defendants specifically market their services to foreign call centers and foreign VoIP carriers looking to transmit high volumes of robocalls to individuals in the United States. The TollFreeDeals website states "TollFreeDeals.com is your premier connection for call center and dialer termination. We are always looking for the best call center routes in the telecom industry. We specialize in short call duration traffic or call center traffic. We understand there is a need for it and we want to help you find all the channels you need!"

[7] Short-duration and unanswered calls include calls where recipients immediately hang up and calls that do not connect, because robocalls are sent to numerous telephone numbers that are not in service.

27. The FAQs on the TollFreeDeals website state, "Do you handle CC (Call Center)/Dialer Traffic? Yes – unlike many carriers we will handle your dialer and call center VoIP termination minutes. If you are looking for USA Dialer, Canada Dialer, or Australia Dialer please fill out our online interop form to test our routes."

28. Defendants regularly transmit massive volumes of short duration calls. For example, over 23 days in May and June of 2019, TollFreeDeals transmitted more than *720 million* calls. Of those calls, more than 425 million, or 59% of the total calls, lasted less than one second in duration. In the telecommunications industry, high volumes of short-duration and unanswered calls are indicative of robocalls that are unwanted by the recipients, often because they are fraudulent. More than 24 million of those calls were placed to phone numbers with area codes in the Eastern District of New York. As Defendants' phone records show the ultimate destination number of every VoIP call they transmit, Defendants know they transmit fraudulent calls to potential victims in the Eastern District of New York.

29. During May and June of 2019, the Palumbos facilitated the delivery of more than 182 million calls through TollFreeDeals from a single India-based VoIP carrier co-conspirator to phones in the United States. One thousand different source numbers (the number from which a call is placed, and that shows up on the recipient's caller ID) accounted for more than 90% of those calls. According to data obtained from a robocall blocking company about calls identified as fraudulent robocalls in 2019, 79% of those 1000 source numbers have been identified as sending fraudulent robocalls. Consequently, TollFreeDeals transmitted an estimated 143 million fraudulent robocalls on behalf of that single India-based co-conspirator during May and June of 2019. Of those calls, an estimated 20% were Social Security imposter calls, 35% were loan

approval scams, and 14% were Microsoft refund scams. The remaining calls were a mixture of IRS imposter, U.S. Treasury imposter, miscellaneous tech support imposter and other schemes.

30. Defendants' knowledge of the fraudulent nature of the telephone calls they deliver to potential victims on behalf of their co-conspirators is also evidenced by the numerous complaints, inquiries, and warnings regarding fraudulent robocalls that Defendants received from other telecommunications carriers and a telecommunications industry trade association since at least 2017. Despite receiving these complaints, inquiries, and warnings, Defendants nevertheless continued to transmit massive volumes of fraudulent robocalls from their co-conspirators to potential victims in the United States.

31. For example, in May 2017, AT&T notified Nicholas Palumbo that it had traced back to TollFreeDeals robocalls received by its customers that spoofed phone numbers belonging to USCIS and the Office of the Inspector General of the U.S. Department of Homeland Security ("DHS-OIG"). AT&T informed Nicholas Palumbo that the callers who spoke to AT&T's customers impersonated U.S. Immigration Officers, and that AT&T had confirmed with USCIS and DHS-OIG that those agencies did not use any of the phone numbers at issue as a legitimate outbound caller ID. Nicholas Palumbo responded that the calls were transmitted to TollFreeDeals from an India-based VoIP carrier, and that he had blocked those two specific phone numbers. Blocking specific numbers is an ineffective means to stop fraudsters who are willing and have the ability to spoof any number as the caller ID number for their fraud calls.

32. In February 2019, AT&T notified Nicholas Palumbo that it had traced back 19 separate calls to AT&T customers that spoofed a USCIS phone number in order to "extort money from our customers." In Nicholas Palumbo's response to AT&T, he acknowledged that those calls were transmitted to TollFreeDeals from the same India-based VoIP carrier that had

transmitted spoofed USCIS calls in 2017. Despite repeated warnings from AT&T that this foreign VoIP carrier was transmitting fraudulent government-impersonation robocalls, the Palumbos continued transmitting VoIP calls on behalf of this customer through at least as recently as June 2019.

33. The Palumbos have also received numerous warnings from telecommunications industry trade association USTelecom that both TollFreeDeals.com and SIP Retail have transmitted fraudulent robocalls, including government impersonation robocalls.

34. From May 2019 through January 2020, TollFreeDeals received 144 notifications from USTelecom that a fraudulent robocall had been traced back to TollFreeDeals. Of these notifications, 83 referenced SSA imposter fraud calls, 24 referenced Tech Support imposter fraud calls, ten referenced IRS imposter fraud calls, and one referenced USCIS impersonation fraud calls. Each of these emails were sent to Nicholas Palumbo at his @tollfreedeals.com email address. Each email stated that a suspicious call had been traced back to TollFreeDeals's network and provided the call date, time and the source and destination phone numbers, to allow TollFreeDeals to identify the specific call at issue in its call logs (referred to in the industry as "call detail records"). Each email also provided a link to USTelecom's web-based traceback portal, where further information was provided about the specific fraudulent call at issue, included a recording of the fraudulent voicemail message that was sent to the recipient's phone. In every case, either the email itself or the traceback portal included a short description of the type of fraud at issue and the details of the fraudulent robocall campaign, such as:

> Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated voice claims suspicious activity on your social security number; press 1. Calls are from apparently random 8XX numbers or other geographic numbers. Call volume estimated at over a million

per day. Because Caller-ID changes with each call, blocking the ANI ["Automatic Number Identification"[8]] is not effective.

35. After receiving each of these notifications from USTelecom, Nicholas Palumbo logged into the USTelecom portal and provided information regarding the customers of TollFreeDeals that had transmitted the fraudulent calls. Many of these fraudulent calls repeatedly traced back to the same India-based customers of TollFreeDeals.

36. From August 2019 through January 2020, USTelecom also notified SIP Retail of 35 tracebacks of fraudulent robocalls, including 19 tracebacks of SSA impersonation fraud calls, three tracebacks of Tech Support impersonation fraud calls, and one traceback of USCIS Impersonation fraud calls. Those notifications were emailed to help@sipretail.com. Upon information and belief, the Palumbos are the only individuals who monitor email traffic to @sipretail.com domain email addresses. SIP Retail logged into the USTelecom traceback portal and notified USTelecom that all 10 of the SSA impersonation calls were sent to SIP Retail by two India-based companies. Both of these companies were also sending fraudulent SSA imposter call traffic through TollFreeDeals.com, as the Palumbos have been notified by USTelecom on multiple occasions.

37. Further, Defendants regularly receive payment from their customers in the form of substantial cash deposits directly into Ecommerce's bank account, from locations throughout the United States raising red flags about the nature of the business of Defendants' customers.

B. Defendants Provide Toll-Free Services for Robocall Schemes

38. Not only do Defendants knowingly pass fraudulent robocalls by the millions into the U.S. telephone system, but they also provide return-calling services to fraudsters so that

[8] ANI refers to the origination telephone number from which a call is placed.

potential victims can call them back. These toll-free telephone numbers and related services are provided in the robocall message as call-back numbers, and appear to be U.S. telephone numbers and thus enable fraudsters to further deceive individuals about the robocall's origin and the identities and locations of the fraudsters at the other end of the call. In reality, what appears to the individual to be a U.S. telephone number is just a telephone number that Defendants register to an internet address designated by the fraudsters. Thus, the toll-free numbers can be used to ring telephones anywhere in the world.

39. While toll-free numbers used for return-calling purposes cannot be "spoofed" like outgoing robocalls, the use of a U.S. toll-free number in Defendants' robocalls schemes serves much the same purpose as spoofing—deception. The toll-free services provided by Defendants use VoIP technology to direct potential victims' return calls from the United States to the foreign fraudsters' call centers. The Defendants have knowingly provided toll-free numbers and associated calling services to foreign robocall fraudsters.

40. All toll-free numbers in the United States are administered by Somos, Inc., a company designated by the Federal Communications Commission ("FCC") as the national administrator of the U.S. toll-free calling system and its database. Among other functions within the industry, Somos registers "Responsible Organizations," that are authorized to provide toll-free numbers to their customers and to register those numbers in the national registry that the industry uses to direct toll-free telephone traffic. Defendants obtain toll-free numbers on behalf of their customers from one or more Responsible Organizations.

41. On July 31, 2019, an employee of a Responsible Organization sent the message below to Nicholas Palumbo via his @tollfreedeals.com email address:

Hello,

> We received a call yesterday (at 6 pm) that we didn't answer.
> Calling Number: +844[XXXXXXX]
> Requesting to call back: 844-[XXX]-[XXXX]
>
> Please see the attached audio and screenshot of the voicemail transcript. Shut down this user immediately as it was associated with the customer account of [TollFreeDeals customer]. These types of scam calls are prohibited from our network and further fraudulent calls from the same customer account will result in termination of said customer account. The number of 844-[XXX]-[XXXX] has been removed from your account in order to protect the integrity of our network.

The attached audio file of a voicemail message stated:

> tomorrow $399.99 is going to be deducted from your account for the remainder of your computer services. If you want to cancel the subscription, please press 1 to talk to our cancellation officer. Or you can call us back on our help line number 1-844-[XXX]-[XXXX]. I'll repeat the help line number 1-844-[XXX]-[XXXX]. Thank you."

42. Over the course of the next two weeks, employees of the Responsible Organization sent an additional six emails to Nicholas Palumbo, notifying him that the Responsible Organization was removing eight additional toll-free numbers from the accounts of two TollFreeDeals customers, because those numbers had been shown to be used in Tech Support impersonation scams and scams impersonating Amazon customer service. In response to each email, Nicholas Palumbo responded simply that he had let the customer of TollFreeDeals know.

43. On August 12, 2019, an employee of the Responsible Organization emailed Nicholas Palumbo and stated:

> Good afternoon Nick,
>
> I wanted to reach out to inform you that we have disabled the account of [TollFreeDeals customer] due to fraudulent complaints. Unfortunately, we do get a lot of complaints about customers under your reseller account. Our first line of defense when issues like arise we deactivate the customer's account. I am informing you that if we do receive any additional complaints about any of your other customers under your re-seller account, we will be forced to deactivate your account.

Nicholas Palumbo responded "I let him know," then responded further, "I will be porting clients over[.] Can't take that chance." In the telecommunications industry, to "port a number" means to move an existing phone number from one provider to another. In effect, Nicholas Palumbo was stating that he planned to take the toll-free numbers registered to his customers through the Responsible Organization who had warned him about fraudulent calls, and move those same numbers to another provider on behalf of his customers.

HARM TO VICTIMS

44. Defendants' fraudulent schemes have caused substantial harm to numerous victims throughout the United States, including many victims located in the Eastern District of New York. It is estimated that Defendants and their foreign co-conspirators defrauded victims out of millions of dollars per year through fraudulent robocalls and return-calling services. If allowed to continue, these losses will continue to rise and result in further harm to victims.

45. In addition to the massive cumulative effect of these fraud schemes on victims throughout the United States, the harm can be devastating to individual victims. Victims have faced terrifying threats from fraudsters impersonating government officials and have lost substantial sums of money.

46. Defendants' fraudulent schemes are ongoing and wide-ranging. Absent injunctive relief by this Court, the Defendants will continue to cause injury to victims in this District and throughout the United States, and the victims' losses will continue to mount.

COUNT I

(18 U.S.C. § 1345 – Injunctive Relief)

47. The United States realleges and incorporates by reference paragraphs 1 through 46 of this Complaint as though fully set forth herein.

48. By reason of the conduct described herein, Defendants violated, are violating, and are about to violate 18 U.S.C. §§ 1343 and 1349 by executing or conspiring to execute schemes or artifices to defraud, or for obtaining money or property by means of false or fraudulent pretenses with the intent to defraud, and in so doing, transmitting or causing to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, writings, signs, signals, pictures, or sounds for the purpose of executing such schemes or artifices.

49. Upon a showing that Defendants are committing or about to commit wire fraud, conspiracy to commit wire fraud, or both, the United States is entitled, under 18 U.S.C. § 1345, to a temporary restraining order, a preliminary injunction, and a permanent injunction restraining all future fraudulent conduct and any other action that this Court deems just in order to prevent a continuing and substantial injury to the victims of fraud.

50. As a result of the foregoing, Defendants' conduct should be enjoined pursuant to 18 U.S.C. § 1345.

PRAYER FOR RELIEF

WHEREFORE, the plaintiff United States of America requests of the Court the following relief:

A. That the Court issue an order, pursuant to 18 U.S.C. § 1345, pending a hearing and determination on the United States' application for a preliminary injunction, that Defendants, their agents, officers and employees, and all other persons and entities in active concert or participation with them are temporarily restrained from:

i. committing and conspiring to commit wire fraud, as defined by 18 U.S.C. §§ 1343 and 1349;

ii. providing, or causing others to provide call termination services for calls terminating in the United States or carrying any VoIP calls terminating in the United States;

iii. providing toll-free telephone services for calls originating in the United States, including providing toll-free phone numbers to other individuals or entities;

iv. destroying, deleting, removing, or transferring any and all business, financial, accounting, call detail, and other records concerning Defendants' operations and the operations of any other corporate entity owned or controlled, in whole or in part, by Defendants.

B. That the Court further order, pursuant to 18 U.S.C. § 1345, that within two days from Defendants' receipt of this Temporary Restraining Order and Order to Show Cause, Defendants shall provide copies of this Temporary Restraining Order and Order to Show Cause to all of their customers for whom they provide (1) United States call termination services, (2) United States toll-free call origination services; and to all entities (a) with whom Defendants have a contractual relationship for automated or least-cost call routing, or (b) from whom Defendants acquire toll-free numbers. Within four days from Defendants' receipt of the Temporary Restraining Order and Order to Show Cause, Defendants shall provide proof of such notice to the Court and the United States, including the names and addresses or email addresses of the entities and/or individuals to whom the notice was sent, how the notice was sent, and when the notice was sent.

C. That the Court further order, pursuant to 18 U.S.C. § 1345, Somos, Inc., in its capacity as the entity designated by the Federal Communications Commission to administer the U.S. toll-free calling system and its database, to temporarily suspend all toll-free numbers registered by or on behalf of any Defendant in this matter, until further order of this Court.

D. That the Court further order, pursuant to 18 U.S.C. § 1345, that any Toll-Free Service Provider that receives notice of this Temporary Restraining Order and Order to Show Cause and has a contractual relationship with one of the Defendants in this matter to provide toll-free numbers, shall provide to Somos, Inc. a list of all toll-free numbers provided to that Defendant that are currently active.

E. That the Court further order, pursuant to 18 U.S.C. § 1345, that any individual or entity who has obtained a toll-free number through one of the Defendants in this matter, either directly or through another intermediate entity, and wishes to continue using that toll-free number may submit a request to the Court, copying counsel for the United States, and identifying: (1) the individual or entity's name, address, phone number, email address, website URL, and the nature of their business; (2) the end-user of the toll-free number's name, address, phone number, email address, and website URL if the end-user did not obtain the toll-free number directly from Defendants; (3) the nature of the end-user's business; (4) the purpose for which the end-user utilizes the toll-free number; (5) the date on which the individual or entity obtained the toll-free number and, if applicable, provided it to the end-user; and (6) whether the toll-free number is used by the individual, entity, or end-user in connection with robocalls. The United States shall then notify the Court within four

business days whether the United States has any objection to removing the specifically identified toll-free number from the list of suspended numbers.

F. That the Court issue a preliminary injunction on the same basis and to the same effect.

G. That the Court issue a permanent injunction on the same basis and to the same effect.

H. That the Court order such other and further relief as the Court shall deem just and proper.

Dated: January 28, 2020

Respectfully submitted,

RICHARD P. DONOGHUE
United States Attorney

DARA OLDS
BONNI J. PERLIN
Assistant United States Attorneys
Eastern District of New York
271-A Cadman Plaza East
Brooklyn, New York 11201
Tel. (718) 254-7000
Fax: (718) 254-6081
dara.olds@usdoj.gov
bonni.perlin@usdoj.gov

JOSEPH H. HUNT
Assistant Attorney General
Civil Division
United States Department of Justice

DAVID M. MORRELL
Deputy Assistant Attorney General

GUSTAV W. EYLER
Director
Consumer Protection Branch

JILL P. FURMAN
Deputy Director

ANN F. ENTWISTLE
CHARLES B. DUNN
Trial Attorneys
U.S. Department of Justice
P.O. Box 386
Washington, D.C. 20044
Tel. (202) 307-0066
Tel. (202) 305-7227
Fax: (202) 514-88742
Ann. F. Entwistle@usdoj.gov
Charles.B.Dunn@usdoj.gov

JS 44 (Rev. 02/19)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

UNITED STATES OF AMERICA

(b) County of Residence of First Listed Plaintiff _____
(EXCEPT IN U.S. PLAINTIFF CASES)

CV 20 - 473

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Dara Olds, Bonni Perlin
U.S. Attorney's Office, Eastern District of New York
271-A Cadman Plaza East, 7th Fl., Brooklyn, NY 11201; (718) 254-7000

DEFENDANTS
NICHOLAS PALUMBO, NATASHA PALUMBO, ECOMMERCE NATIONAL, LLC d/b/a Tollfreedeals.com, and SIP RETAIL d/b/a sipretail.com

County of Residence of First Listed Defendant Maricopa
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

FILED
IN CLERK'S OFFICE
U.S. DISTRICT COURT E.D.N.Y.
★ JAN 28 2020 ★
BROOKLYN OFFICE

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☒ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

KORMAN, J.
MANN. M.J.

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated or Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☒ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
Request for relief pursuant to 18 U.S.C § 1345

Brief description of cause:
Violations of wire fraud statutes, 18 U.S.C. §§ 1343, 1349

VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☐ Yes ☒ No

VIII. RELATED CASE(S) IF ANY *(See instructions)*:

JUDGE _____ DOCKET NUMBER _____

DATE
January 28, 2020

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

CERTIFICATION OF ARBITRATION ELIGIBILITY

Local Arbitration Rule 83.7 provides that with certain exceptions, actions seeking money damages only in an amount not in excess of $150,000, exclusive of interest and costs, are eligible for compulsory arbitration. The amount of damages is presumed to be below the threshold amount unless a certification to the contrary is filed.

Case is Eligible for Arbitration ☐

I, Dara Olds, counsel for United States of America, do hereby certify that the above captioned civil action is ineligible for compulsory arbitration for the following reason(s):

☐ monetary damages sought are in excess of $150,000, exclusive of interest and costs,

☑ the complaint seeks injunctive relief,

☐ the matter is otherwise ineligible for the following reason

DISCLOSURE STATEMENT - FEDERAL RULES CIVIL PROCEDURE 7.1

Identify any parent corporation and any publicly held corporation that owns 10% or more or its stocks:

RELATED CASE STATEMENT (Section VIII on the Front of this Form)

Please list all cases that are arguably related pursuant to Division of Business Rule 50.3.1 in Section VIII on the front of this form. Rule 50.3.1 (a) provides that "A civil case is "related" to another civil case for purposes of this guideline when, because of the similarity of facts and legal issues or because the cases arise from the same transactions or events, a substantial saving of judicial resources is likely to result from assigning both cases to the same judge and magistrate judge." Rule 50.3.1 (b) provides that " A civil case shall not be deemed "related" to another civil case merely because the civil case: (A) involves identical legal issues, or (B) involves the same parties." Rule 50.3.1 (c) further provides that "Presumptively, and subject to the power of a judge to determine otherwise pursuant to paragraph (d), civil cases shall not be deemed to be "related" unless both cases are still pending before the court."

NY-E DIVISION OF BUSINESS RULE 50.1(d)(2)

1.) Is the civil action being filed in the Eastern District removed from a New York State Court located in Nassau or Suffolk County? ☐ Yes ☑ No

2.) If you answered "no" above:
a) Did the events or omissions giving rise to the claim or claims, or a substantial part thereof, occur in Nassau or Suffolk County? ☐ Yes ☑ No

b) Did the events or omissions giving rise to the claim or claims, or a substantial part thereof, occur in the Eastern District? ☑ Yes ☐ No

c) If this is a Fair Debt Collection Practice Act case, specify the County in which the offending communication was received:

If your answer to question 2 (b) is "No," does the defendant (or a majority of the defendants, if there is more than one) reside in Nassau or Suffolk County, or, in an interpleader action, does the claimant (or a majority of the claimants, if there is more than one) reside in Nassau or Suffolk County? ☐ Yes ☐ No

(Note: A corporation shall be considered a resident of the County in which it has the most significant contacts).

BAR ADMISSION

I am currently admitted in the Eastern District of New York and currently a member in good standing of the bar of this court.

☑ Yes ☐ No

Are you currently the subject of any disciplinary action (s) in this or any other state or federal court?

☐ Yes (If yes, please explain ☑ No

I certify the accuracy of all information provided above.

Signature: Dara A Olds

Last Modified: 11/27/2017

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

Plaintiff,

v.

NICHOLAS PALUMBO, NATASHA PALUMBO, ECOMMERCE NATIONAL, LLC d/b/a Tollfreedeals.com, and SIP RETAIL d/b/a sipretail.com,

Defendants.

CV 20 - 473

Civil Action No.

KORMAN, J.

MANN. M.J.

DECLARATION OF SAMUEL BRACKEN

I, Samuel Bracken, have personal knowledge of the facts set forth below, and if called as a witness I would testify as follows:

1. I have been a Postal Inspector with the United States Postal Inspection Service ("USPIS") since February 2004. I am currently assigned to the Elder Fraud Task Force at the Department of Justice, Consumer Protection Branch. I am assigned to investigate violations of federal law, including mail fraud and wire fraud, in violation of Title 18, United States Code, Sections 1341 and 1343, respectively. I have received training in investigating elder fraud, social security fraud, IRS fraud, identity theft, credit card fraud, counterfeit check fraud, counterfeit identification card fraud, mail, and wire fraud offenses, including attending seminars and conferences hosted by the Inspection Service, the United States Department of Justice, the International Association of Financial Crimes Investigators, and various other law enforcement entities. During my employment as an Inspector, I have participated in hundreds of

investigations involving identity fraud, aggravated identity theft, mail fraud and wire fraud. In addition, I have been the Inspection Service's case agent on numerous investigations involving these offenses.

2. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation, information from other individuals including other law enforcement officers, complainants, and other parties, witness interviews, and my review of documents, public records, USPIS records, and other sources. Because this declaration is submitted for the limited purpose of establishing probable cause in support of the application for a temporary restraining order, it does not set forth each and every fact that I learned during the course of this investigation.

SUSPICIOUS PAYMENTS TO TOLLFREEDEALS

3. In the course of this investigation, records were obtained from Wells Fargo Bank regarding an account held in the name of Ecommerce National LLC with a signer of Nicholas Palumbo. For the time period of May 28, 2019 through September 11, 2019, the account received nineteen cash deposits totaling $130,250.00. These deposits occurred in locations across the United States, including in Minnesota, South Carolina, Florida, Alabama, and New Jersey. None of these cash deposits occurred in Arizona, the principle location of business for Ecommerce National.

4. Within days of receiving these cash deposits, Nicholas Palumbo would transfer the funds from the Wells Fargo Account, via wire transfers or checks maybe payable to Ecommerce National LLC, to two accounts held in the name of Ecommerce National LLC at JP Morgan Chase. The sixteen transactions totaled $131,584.00.

5. Through my training and experience, I know that accounts known as "interstate funnel accounts" are one of the most efficient means for criminal orgnanizations to rapidly move illicit proceeds within the U.S. and abroad. Based on my training as a federal law enforcement officer and fraud investigator, I know that funnel accounts offer the rapid movement of money across great distances with minimal fees and the anonymity of the depositors, since the deposits are usually under the reporting thresholds. Analysis of Bank Secrecy Act (BSA) reporting has identified that the following account activity is often associated with funnel accounts:

- out-of-state, anonymous cash deposits in multiple states;
- rapid cash withdrawals for amounts similar to cash deposits;
- use of counter deposit slips;
- individual deposits and withdrawals intentionally under $10,000 (structuring);
- limited account credits besides cash deposits (i.e., no payroll, wire transfers);
- no legitimate business purpose evident;
- and deposit activity greater than expected income.

Based on my training and experience, it appears that TollFreeDeals is utilizing the Wells Fargo bank account as a funnel account to receive fraud proceeds from co-conspirators.

NEW YORK VICTIMS OF DEFENDANTS' FRAUDULENT ROBOCALLING CONSPIRACIES

6. On January 16, 2020, I interviewed victim J.K., an 84-year-old man who is a former member of the United States Marine Corps and who resides in Belle Harbor, New York. J.K. was the victim of a social security imposter scam. J.K. received a message on his cellular telephone on May 23, 2019, concerning his social security number. J.K. called back the phone number left in the message, 512-XXX-XXXX, and spoke with an individual who stated that he

was from the U.S. Marshals Service and that a warrant had been issued for J.K.'s arrest. He then transferred J.K. to a man named who claimed his name was "David" and that he was an employee with the Social Security Administration ("SSA"). David told him that a car had been rented in Houston, Texas using J.K.'s personal information, including his social security number, and that the car was found by local police with evidence of drugs and money laundering. J.K. was told there was a warrant for his arrest based on this activity.

7. David told J.K. he would help J.K. to straighten this situation out, and that J.K. needed to protect his bank accounts from forfeiture and that the government was going to seize his funds due to the criminal activity. David asked J.K. about his bank accounts, and directed J.K. to wire transfer all of the money out of his account to an account number David provided. David informed J.K. that his money was being wired to the U.S. Marshals Service, who would provide his money back to him at a later date after the situation with the warrant was cleared up. J.K. proceeded to transfer $9,800.00 from his bank account to the account provided by David. J.K. spent several hours on the phone during this interaction. J.K. became suspicious after he wired the money, told David he would not be sending any more, and ended the phone call.

8. J.K. then received a call from an individual claiming to be with the warrant squad of the New York City Police Department (NYPD). The individual claiming to be from the NYPD told J.K. that in order to get the warrant lifted, J.K. needed to call David back. J.K. received several more calls, but he did not answer them. J.K. contacted his bank in an attempt to stop the wire transfer, and was told that the money had already been removed from the account to which it was sent.

9. I reviewed call detail records obtained from TollFreeDeals, and confirmed that multiple calls were made to J.K.'s cell phone on May 23, 2019. All of the calls spoofed the main

SSA toll-free customer service number, and were all sent to TollFreeDeals by the same India-based VoIP carrier.

10. On January 16, 2020, I spoke with C.E., who was a victim of an SSA impersonation scam. C.E. is a 36-year-old man who recently received U.S. citizenship and resides in Brooklyn, New York. C.E. received a telephone call on June 6, 2019, from a man who claimed his name was "George" and that he was from SSA. George told C.E. that SSA was investigating his name and social security number being used in connection with money laundering. George told C.E. that there was a warrant out for his arrest, and George already knew C.E.'s social security number. George told C.E. that the next step he needed to take to protect himself was to file a report with a police officer. George then connected C.E.'s phone call with a man claiming to be a police officer.

11. The police officer told C.E. that he had to secure his bank accounts by moving the money out of his accounts, so the money wouldn't be seized. The police officer instructed C.E. to go to Best Buy and purchase gift cars using his debit card to remove the money from his bank account. C.E., who was working as a driver for Uber, then drove to a Best Buy in Queens, New York, where he purchased two Hotels.com gift cards with a combined value of $700.00. He then provided the gift card numbers to the man on the phone. The man on the phone then requested more money, but C.E. didn't have any more money in his bank accounts. After he got off the phone, C.E. realized he had been scammed, and he filed a police report and a complaint with the Federal Trade Commission ("FTC"). C.E. stated that he received another call from the same people later that day, and the caller told him that they would be coming to his apartment to provide him with his new social security number.

12. I reviewed call detail records obtained from TollFreeDeals, and confirmed that a call to C.E.'s phone lasting almost two hours was sent through TollFreeDeals on June 6, 2019, from India-based VoIP carrier Company A.

13. I have also reviewed a complaint filed with the Federal Trade Commission by L.U., a man in his forties who resides in Roosevelt, New York, in Nassau County. L.U. reported to the FTC that he received a call on June 5, 2019, from 877-382-4357. That is the phone number of the FTC's Consumer Response Center. On the FTC's website, FTC states that while they receive inbound calls at that number, FTC does not make outbound calls from that number. L.U. reported that the person who called him posed as the SSA, and informed L.U. that his social security number was going to be suspended due to criminal activity if he did not provide his personal information. L.U. reported that he lost $2,200.00 as a result of this SSA imposter scam.

14. I have reviewed call detail records obtained from TollFreeDeals, and confirmed that two calls were sent from Company A through TollFreeDeals to L.U.'s phone number on June 5, 2019. Both calls spoofed FTC's Consumer Response Center as the source number.

Pursuant to 28 U.S.C. § 1746, I hereby declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief. Executed on January 27, 2020, in Phoenix, Arizona.

Samuel Bracken, Postal Inspector
United States Postal Inspection Service

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

Plaintiff,

v.

NICHOLAS PALUMBO, NATASHA PALUMBO, ECOMMERCE NATIONAL, LLC d/b/a Tollfreedeals.com, and SIP RETAIL d/b/a sipretail.com,

Defendants.

CV 20 - 473
Civil Action No.

KORMAN, J.

MANN. M.J.

DECLARATION OF MARCY RALSTON

I, Marcy Ralston, have personal knowledge of the facts set forth below, and if called as a witness I would testify as follows:

1. I have been a Special Agent with the Social Security Administration's Office of Inspector General ("SSA OIG"), Office of Investigations since October 2004. I have been employed as a federal law enforcement officer for approximately 16 years. From approximately August 2002 until December 2003, I was employed as a Postal Inspector with the United States Postal Inspection Service. My current duties include investigating violations of Federal and State laws, primarily as they relate to misuse of social security numbers and violations of laws and regulations administered by the SSA. This includes crimes of mail fraud, identity deception, welfare fraud, theft, perjury and forgery. I have participated in multiple search warrants. I have worked several large scale, multi-agency investigations and have interviewed multiple witnesses, suspects and cooperating individuals as a part of my duties. Before this, I received a Bachelor's Degree from Indiana University in Criminal Justice in 1997. I have attended twelve weeks of

federal law enforcement training from the Inspection Service, as well as continuing education with SSA-OIG.

2. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation, information from other individuals including other law enforcement officers, complainants, and other parties, witness interviews, and my review of documents, public records, USPIS records, and other sources. Because this declaration is submitted for the limited purpose of establishing probable cause in support of the application for a temporary restraining order, it does not set forth each and every fact that I learned during the course of this investigation.

3. SSA Imposter fraud has resulted in the filing of hundreds of thousands of complaints with the Administration in just the last fifteen months. Specifically, analysis of our complaints database reveals 465,000 complaints about fraudulent telephone impersonation of the Administration between October I, 2018 and September 30, 2019; these complaints reflect aggregated losses of over $14 million.

4. In addition, the Federal Trade Commission ("FTC") collects complaints in its Consumer Sentinel database on SSA and other government imposter scams. For 2018, the FTC received more than 39,000 fraud complaints about SSA imposters, with related victim losses of approximately $11.5 million. SSA imposter fraud complaints for 2019 include approximately 166,000 complaints relating more than $37 million in losses.[1] In my experience, these complaint

[1] Regarding government imposter fraud more broadly and not limited just to SSA imposters, the FTC's Consumer Sentinel database contains 255,223 complaints reflecting $128,479,054 in losses for 2018, and 389,563 complaints reflecting $152,946,623 in losses for 2019.

numbers substantially underrepresent the extent of fraudulent activity because most victims do not report their losses to the government.

OVERVIEW OF DEFENDANTS' WIRE FRAUD SCHEME

5. This investigation involves a wire fraud scheme conducted and facilitated by husband and wife Nicholas and Natasha Palumbo ("the Palumbos") through the entities Ecommerce National LLC d/b/a TollFreeDeals.com ("TollFreeDeals") and SIP Retail, LLC d/b/a SIPRetail.com ("SIP Retail") (collectively, "Defendants"). The Palumbos operate and control the named entities from their home in Paradise Valley, Arizona.

6. As relevant to this Declaration, "robocalling" refers to an automated process of placing large volumes of telephone calls over the internet in order to deliver recorded messages, in contrast to calls placed one at a time by a live person. SSA OIG is investigating criminal schemes perpetrated by individuals operating one or more call centers located in India and other foreign locations. Fraudsters at the call centers impersonate government agencies and other entities – including the SSA, other government agencies, and businesses – and place millions of robocalls to phones in the United States. These robocalls convey recorded messages instructing the recipients to contact the impersonated entity regarding problems with their social security numbers, missed court dates, imminent asset freezes, and other such lies that are intended to secure the recipient into establishing phone contact with a criminal. In all of these schemes, the criminals attempt to defraud and extort money from anyone who contacts them in response to their messages.

7. Since at least 2016, despite repeated warnings from various government entities and industry actors, the Palumbos and the entities they control have provided robocallers with unfettered access to the U.S. phone system and thus the ability to deluge U.S. residents with

millions of fraudulent robocalls. The Palumbos, through their companies, have also provided fraudsters with toll-free phone numbers used in furtherance of the robocall fraud schemes that allow victims to return calls to the fraudsters in foreign locations at what appears to the potential victim to be a legitimate U.S. toll-free phone number.

8. Defendants' participation in these fraudulent robocall schemes is essential to the success of the schemes. Without someone willing to accept the fraudsters' robocall traffic into the U.S. telephone system, even though the fraudsters have internet access they would be unable to contact any potential victims in the first instance. The Palumbos provide the crucial interface between foreign internet-based phone traffic and the U.S. telephone system, and our investigation reveals that they do so with full knowledge that they are participating in massive frauds. Similarly, by providing toll-free services, Defendants not only enable initial contact with potential victims, but also provide legitimate U.S. toll-free numbers that cloak the fraud in a façade of legitimacy and allow the unwitting to become victims when they return calls to fraudsters after they receive a robocall voicemail message.

9. The robocall imposters in this investigation use a variety of methods to receive funds from victims, including but not limited to asking victims to: purchase gift cards or other stored value cards and transmit the numbers from the back of the cards to the fraudsters; send bank wires; and send cash payments by overnight carrier.

10. Victims will often send these funds to individuals referred to by law enforcement as "money mules" located in the United States, who receive and collect victim payment funds from fraud schemes, and then conduct transactions on behalf of their "handlers," who will instruct them what to do with the funds. "Money mules" will often send money from the United States back to India, via money transmitting businesses, and/or pay the business expenses for the call centers,

including paying U.S. based companies that are helping to route scam calls to U.S. victims. These payments will often consist of cash deposits into the bank accounts of the U.S. based companies.

11. In the course of this investigation, we have learned that TollFreeDeals and SIP Retail have transmitted robocalls as part of numerous fraudulent robocalling schemes, including:

a) SSA Imposters – SSA Imposters send recorded messages falsely claiming that the recipient's social security number has been used in criminal activity, the recipient's social security benefits will be suspended, the recipient failed to appear before a grand jury and faces imminent arrest, or the recipient's social security number will be terminated. When an individual calls back or connects to the fraudster, the fraudster claims to be an SSA employee and typically tells the individual to transfer substantial funds to the SSA for safekeeping until the individual is issued a new social security number, at which point the individual's funds will be returned.

b) Internal Revenue Service ("IRS") Imposters: IRS imposters send recorded messages falsely claiming that the recipient has been implicated in tax fraud, the individual has avoided attempts to enforce criminal laws, the individual has avoided court appearances, or the individual faces imminent arrest. When a recipient calls back or connects to the fraudster, the fraudster claims to be an IRS or Treasury employee and typically tells the recipient to transfer funds to the IRS to resolve various fictitious tax and legal liabilities, or for safekeeping in order to avoid seizure of assets.

c) United States Citizenship and Immigration Services ("USCIS") Imposters: USCIS imposters send recorded messages falsely claiming that the recipient has failed to fill out immigration forms correctly, the recipient faces imminent arrest or

deportation, that the recipient's home country has taken formal action against the recipient that may result in deportation, or the recipient has transferred money in a way that will result in deportation. When a recipient calls back or connects to the fraudster, the fraudster claims to be a USCIS employee and typically tells the recipient to pay various fees or fines to avoid immigration consequences.

d) Tech Support Imposters: Fraudsters operating tech support scams impersonate various well-known tech companies, such as Apple or Microsoft, and send recorded messages falsely claiming that the recipient has computer security problems that require assistance. When an individual connects with the fraudster, the fraudster often convinces the individual to pay for fictitious tech support and computer security services, and to allow the fraudster remote access to the victim's bank accounts.

e) Loan Approval Scams: Fraudsters operating loan approval scams leave messages impersonating a "lender" offering a great, guaranteed rate on a "pre-approved" loan. When a call recipient connects with the fraudster, the fraudster will emphasize that a poor credit history does not matter, and all the call recipient has to do to secure the pre-approved loan is a pay a one-time fee up front.

TECHNOLOGIES USED IN THE ROBOCALLING FRAUD SCHEMES

12. The technical ability to place the fraudulent calls at issue in the investigation is dependent on (1) voice-over-internet-protocol ("VoIP")[2] calling and related technology to create the calls, and (2) a "gateway carrier" to introduce the foreign call traffic into the U.S. phone system.

[2] VoIP stands for voice-over-internet protocol and allows users to place phone calls over a broadband internet connection.

In the telecommunications industry, the term "gateway carrier" refers to a U.S. based person or entity that agrees with a foreign person or entity (often by contract) to accept foreign-source VoIP telephone traffic. VoIP uses a broadband internet connection – as opposed to an analog traditional phone line – to place phone calls locally, long distance, and internationally, without regard to whether the call recipient uses a cellular phone or a traditional wired phone. The technology employed by modern telecommunication providers mediates between digital VoIP signals and regular telephone signals so that communication is seamless between VoIP and non-VoIP users at either end. VoIP is used in the schemes both to place robocalls to U.S. phones and to communicate with individuals who either answer the robocall or call the number contained in the recorded robocall message.

13. VoIP relies upon a set of rules for electronic communication called Session Initiation Protocol ("SIP"). Much like the way browsing websites on the Internet use HyperText Transfer Protocol ("HTTP") to initiate and conduct information exchanges between devices through exchanges of packets of information, SIP is a set of rules used to initiate and terminate live sessions for things such as voice and video communication between two or more points connected to the Internet. Both SIP voice communication and HTTP web-browsing rely on exchanging data packets between two points. For example, web browsing via HTTP requires an individual to request information from another point on the internet, usually by clicking on a hyperlink or entering a web address in a browser's address bar, usually preceded by "http://www," which tells the device that it is making a request for information on the World Wide Web via HTTP. A device receiving that request will send back information to the requesting device, and thus, the requesting device will display the requested website.

14. Similarly, a voice call via SIP starts as a data packet sent to initiate a call, a responsive packet sent back that indicates whether the call has been answered, and numerous other packets transiting back and forth; amongst these data packets is information that machines at either end turn into audible signals, i.e., a conversation that can be heard by the participants. In the case of robocalls, a recorded message is transmitted once the call is answered by a live person or by voicemail.

15. Robocalls should not be understood as traditional telephone calls, but rather, requests for information and responsive data packets transiting the internet via SIP. An outgoing robocall begins as a request for information sent by an automatic telephone dialing system known as an "autodialer" that—in conjunction with VoIP services—enables the caller to make millions of sequential requests for information (i.e., outbound VoIP phone calls) in a very short time. A VoIP autodialer is a specialized type of telecommunications equipment having the capacity to (1) store or produce telephone numbers to be called, and (2) request responsive information from devices at the other end of the call, i.e., dial the telephone numbers. The autodialer's requests for information are directed to devices (here, telephones) that send back responsive information when the call is answered either by a live person or the person's voicemail. When the autodialer receives the information from the called device indicating that the call is answered, the autodialer will then send information back to that device (the phone) in the form of a recorded message. As relevant here, fraudsters created the recorded message that conveys false threats while impersonating a U.S. agency or the other entities described above.

16. A fraudster making these robocalls can not only send a recorded message to the potential victim's phone, but can misrepresent the origin of the call on the call recipient's caller ID. Normally, a recipient's caller ID will display information identifying the caller by means of a

telephone number that is automatically displayed because the caller owns the right to use that phone number; however, many VoIP software packages allow the caller to specify the information appearing on the call recipient's caller ID, much in the same way an email's subject line can be edited to state whatever the sender wishes. This practice of specifying what appears on the recipient's caller ID is called "spoofing." This feature of VoIP technology permits a caller with an illicit motive to spoof a legitimate phone number, such as that belonging to a government entity, in order to cloak the fraudsters with indicia of authority and induce the recipients to answer the call. Spoofing also encourages potential victims to return calls when they look up the spoofed number and see that it is a number used by an official government entity. In these robocalling schemes, spoofing serves the purpose of deceiving the potential victim about who is calling them.

17. Spoofing any phone number is a simple matter of editing an SIP file to state the desired representation on the caller ID. These files can then be loaded into an autodialer to become robocalls, replicated millions of times with the spoofed, fraudulent caller ID information.

18. The fraudulent robocalls generally leave prerecorded, threatening messages for recipients. Some of the fraudulent messages direct the recipient to press a key to speak with a live operator. Other fraudulent messages leave a domestic telephone number as a "call-back" number. In either case, whether the recipient presses a key or calls the call-back number, the recipient will be connected to a fraudster in a foreign call center.

19. A gateway carrier is also essential to these fraud schemes perpetrated through these robocall schemes. Foreign call centers and VoIP carriers cannot connect VoIP phone traffic directly to the U.S. telephone system from a foreign location without the assistance of a U.S.-based telecommunications provider willing to accept the foreign call traffic. For example, a fraudulent call center in India cannot directly upload tens of millions of robocalls to the U.S. telephone

system, even where they have broadband internet and VoIP service. Foreign VoIP telephone traffic cannot enter the U.S. telephone system without travelling through a gateway carrier willing to accept the foreign traffic and introduce it to the U.S. telephone system. In the course of this investigation, SSA OIG has determined that Defendants act as gateway carriers for calls originating abroad that are bound for the United States. In the context of the schemes, fraudulent robocalls are "US terminat[ed]" calls, and return calls to fraudsters in other countries are "international voice terminat[ed]" calls.

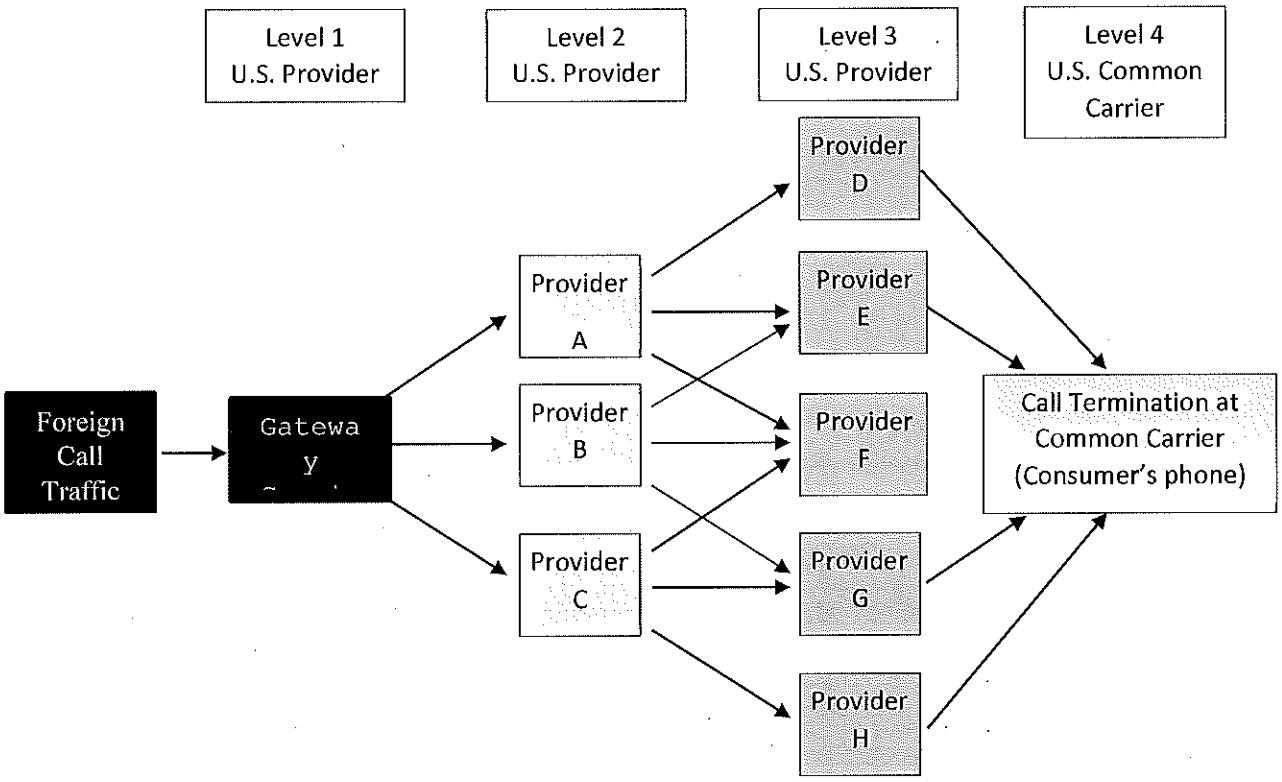
20. In the course of this investigation, I learned that with little more than off-the-shelf VoIP technology, an autodialer, and a business relationship with a gateway carrier, any individual or entity with a broadband internet connection can introduce unlimited numbers of robocalls into the U.S. telephone system from any location in the world.

LEAST-COST CALL ROUTING AND TRACEBACKS

21. When foreign call centers route fraudulent robocalls through Defendants to recipients in the United States through VoIP technology, the calls typically pass through many different VoIP carriers. First, the calls typically pass from a foreign VoIP carrier to Defendants as the U.S. gateway carrier. From Defendants, calls typically pass through multiple other carriers until they reach a common carrier such as AT&T or Verizon. Consumer-facing companies like Verizon and AT&T are known in the industry as "common carriers."

22. With modern telecommunications infrastructure, outbound VoIP calls do not take a defined path from their origin to the final destination. Rather, the system routes calls through automated equipment that determines the lowest possible connection cost at each routing step, depending on preexisting contractual relationships between the various entities. Typically, the company at each routing step will have numerous existing contracts through which it can route

outbound calls through intermediate providers to the common carriers as the last routing step before an individual in the United States can answer the call. This automated routing process is called "least-cost routing," illustrated in the following diagram beginning with a first-level U.S. gateway carrier:



In this simple example, arrows represent possible routing paths between providers based on preexisting contracts. Here, the gateway carrier has three contracts with second-level U.S. providers A, B, and C, each of which in turn has three contracts with third-level providers further into the U.S. phone system (denoted by Providers D, E, F, G, and H). Each of the third-level providers is able to pass calls to the fourth-level common carrier that provides telephone service to the U.S. individual. The call will move through one of many paths, depending on the effective contract terms between the gateway carrier, providers, and common carriers at the time the call is

routed that achieve the lowest cost to transmit the call, i.e., "least-cost routing." In real-world application, least-cost routing may involve more than four levels of U.S. companies.

23. In light of least-cost routing and the prevalence of spoofing telephone numbers, identifying the source of any specific robocall requires a labor-intensive process known in the telecommunications industry as "traceback." In order to conduct the traceback, an investigator must trace backwards each individual "hop" the call took in its least-cost-routing journey from the gateway carrier. For example and referencing the diagram above, the common carrier will be able to query its own system and determine which Level 3 Provider it received the call from, but it will not be able to see beyond that. The common carrier must contact the Level 3 Provider and ask that carrier to determine from its records what Level 2 Provider it received the call from. The common carrier must then contact the Level 2 Provider and ask them to determine which Level 1 provider they received the call from. This process continues at each "hop" until a provider identifies a foreign source – that carrier is then the "gateway carrier" that permitted the foreign telephone traffic to enter the U.S. phone system.

DEFENDANTS' ROLE IN AND KNOWLEDGE OF ROBOCALLING WIRE FRAUD CONSPIRACIES

24. Documents and other evidence obtained and reviewed in the course of this investigation, including Arizona Secretary of State and Arizona Corporation Commission records, the FCC 499 Filer Database, and a review of LinkedIn profiles, have revealed that Nicholas Palumbo has been the Chief Executive Officer of Ecommerce National LLC d/b/a TollFreeDeals.com ("TollFreeDeals") since approximately 2003. Those records further demonstrate that since at least 2016, Nicholas and Natasha Palumbo have operated TollFreeDeals

as a VoIP carrier, originally out of their home in Scottsdale, Arizona, and since mid-2019 out of their current home in Paradise Valley, Arizona.

25. As of January 25, 2020, the TollFreeDeals.com website identifies Nicholas Palumbo as the President/Founder of TollFreeDeals.com, and Natasha Palumbo as the Vice President of Business Development. Through TollFreeDeals, the Palumbos provide inbound VoIP calling to the United States (also known as "U.S. VoIP termination," because the calls "terminate" in the United States) to customers located both here in the United States and abroad. Defendants provide unrestricted VoIP dialing, meaning that they place no restriction on the number of calls their customers can place or the duration of those calls.

26. Through TollFreeDeals, the Palumbos specifically cater to call centers placing robocalls. The company's website states, "TollFreeDeals.com is your premier connection for call center and dialer termination. We are always looking for the best call center routes in the telecom industry. We specialize in short call duration traffic or call center traffic. We understand there is a need for it and we want to help you find all the channels you need!" The "FAQs" page of the website states, "Do you handle CC (Call Center)/Dialer Traffic? Yes – unlike many carriers we will handle your dialer and call center voip termination minutes." The website header also contains the statement "Call Center Minutes Terminated," followed by a number that updates every few seconds. As of January 23, 2020, that number was 10,491,500,323. Based on SSA OIG's investigation and as described above, all foreign fraudsters committing SSA impersonation fraud, as well as other government impersonation fraud and tech support impersonation fraud utilize robocalls and call centers. Defendants specifically market their U.S. call termination services to these types of customers.

27. A review of Arizona Corporation Commission records revealed that Natasha Palumbo is the registered owner and CEO of SIP Retail LLC, and has served in this capacity since registering the company on August 29, 2017. Arizona Corporation Commission records also reveal that Nicholas Palumbo is an officer/agent of SIP Retail, and that SIP Retail's current statutory agent address is the same as that for TollFreeDeals – the Palumbos' current home address in Paradise Valley, Arizona. I also viewed the website for SIP Retail, which lists Natasha Palumbo as the CEO and Founder and offers VoIP call termination services into the United States, just like TollFreeDeals. SIP Retail's website is nearly identical to the website for TollFreeDeals, including listing the same phone number for customer inquiries.

28. The websites for both TollFreeDeals and SIP Retail state that the companies use the switching platform Sip Navigator to carry VoIP termination traffic.

29. Over the past two years, Defendants received many notices, inquiries, warnings, complaints, and subpoenas concerning fraudulent robocalls transiting their systems. These warnings and inquiries came from other telecommunications companies, an industry trade group, and law enforcement agencies. Further, a review of the call detail records in the Palumbos' possession reveals that the call traffic transmitted by the majority of their customers is filled with the indicia of fraud. Nevertheless, Defendants continue to enable these massive fraud schemes to be perpetrated on U.S. individuals.

Warnings and Traceback Requests from USTelecom

30. USTelecom is a nonprofit trade association for the U.S. broadband and communications industry. USTelecom has developed an Industry Traceback Group across the telephonic communications industry to trace robocalls to their sources. Based on tracebacks

conducted with the assistance of the Industry Traceback Group, SSA OIG has identified TollFreeDeals as the number one gateway carrier of SSA imposter calls in 2019.

31. When the Industry Traceback Group conducts a traceback of a fraudulent robocall, USTelecom sends a series of email messages, starting with the common carrier whose customer received the fraudulent robocall, and getting information from each VoIP carrier in the chain about who sent the call to that VoIP carrier. These emails are referred to below as "traceback emails."

32. The Palumbos received USTelecom traceback emails about fraudulent calls that had been transmitted through TollFreeDeals and SIP Retail. Every USTelecom traceback email stated that a suspicious call has been traced back to TollFreeDeals or SIP Retail and provided the call date and time, the source number (the number that appears on the call recipient's caller ID, as well as in the gateway carrier's call records as the source of the call) and the call recipient's phone number to allow TollFreeDeals or SIP Retail to identify the specific call at issue in its call detail records. Each email also provided a link to USTelecom's web-based traceback portal, where further information is provided about the specific fraudulent call at issue, including a recording of the fraudulent voicemail message that was left on a recipient's voicemail. USTelecom traceback emails were sent to the Palumbos at nick@tollfreedeals.com or to help@sipretail.com.

33. Each traceback email from USTelecom included a short description of the type of fraudulent robocall at issue and the details of the fraudulent robocall campaign. Prior to August 2019, those descriptions were included in the traceback portal, but beginning in August 2019, those descriptions were also included in the text of the traceback email itself. An example of a traceback email sent to TollFreeDeals on August 14, 2019, is attached hereto as Exhibit 1. That email includes the following description of the fraud scheme:

> Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated voice claims suspicious activity on your social security number; press 1. Calls are from apparently random 8XX numbers or other geographic numbers. Call volume estimated at over a million per day. Because Caller-ID changes with each call, blocking the ANI is not effective.

The abbreviation "ANI "stands for "Automatic Number Identification," and for these purposes refers to the purported source number. Evidence obtained in this investigation indicates that, in response to traceback emails, Defendants blocked the single source number identified in the each email.

34. The traceback emails include a hyperlink that when clicked leads to USTelecom's online traceback portal, specifically, to a page with information regarding the specific fraudulent robocall that was the subject of the email. The portal includes audio of the voicemail message left as part of this SSA imposter robocalling campaign. I listened to the recorded audio linked to a call transmitted by TollFreeDeals on December 19, 2019, which states:

> We have been forced to suspend your social security number with immediate effect. Due to this, all your social benefits will be cancelled until further clearance. In case you feel this is due to an error, you may connect with legal [unintelligible] Social Security Administration. In order to connect with a Social Security Administration officer, press one now. In case we do not hear from you your social will be blocked permanently. To connect with the officer now, press 1 and you will automatically be connected with the concern departments. We did not receive any input. Dear citizen, in order to speak with Social Security personal regarding your social security, press 1 and this automated system will connect you with the officials. Press….

35. On June 3, 2019, USTelecom sent a traceback email to TollFreeDeals regarding an SSA imposter call. A consultant hired by USTelecom named David Frankel then corresponded directly with Nicholas Palumbo regarding the original SSA impersonation call traceback. In response, Nicholas Palumbo identified Company A, an India-based telecommunications company,

as the provider that had transmitted the SSA impersonation call to TollFreeDeals. In further email correspondence over the course of the day, David Frankel identified several different calls that were all part of the same SSA impersonation fraud campaign and all appeared on caller-ID to be coming from different source numbers. Nicholas Palumbo identified all seven calls as having been transmitted to TollFreeDeals by Customer A.

36. Three days after this email exchange, victim C.E. who was later interviewed by the Postal Inspection Service, was defrauded by an SSA imposter call. TollFreeDeals call detail records show that the SSA imposter call was transmitted from Company A to TollFreeDeals and eventually to victim C.E.'s cell phone. *See* Declaration of Samuel Bracken, Postal Inspector with the United States Postal Service, dated January 27, 2020, ¶¶ 10-12.

37. Based on the volume of traceback emails that TollFreeDeals and SIP Retail have received from USTelecom, Defendants were warned repeatedly that many of their customers were transmitting millions of fraudulent robocalls. From May 2019 through January 2020, TollFreeDeals received a total of 144 notifications from USTelecom that a fraudulent robocall had been traced back to TollFreeDeals. Of these notifications, 83 referenced SSA imposter fraud calls, 24 referenced Tech Support imposter fraud calls, ten referenced IRS imposter fraud calls, and one referenced a USCIS impersonation fraud call. TollFreeDeals reported to USTelecom that it had received these 144 calls from 14 different customers, and that all of the SSA Impersonation calls traced back to the same two Indian entities.

38. From August 2019 through December 2019, USTelecom notified SIP Retail of 35 tracebacks of fraudulent robocalls, including 19 tracebacks of SSA impersonation fraud calls, six tracebacks of Tech Support fraud calls, and one traceback of USCIS impersonation fraud calls. SIP Retail reported back to USTelecom that it had received these 35 fraudulent calls from seven

different companies, and that all 19 of the SSA impersonation calls were sent to SIP Retail by two India-based companies that sent SSA imposter calls through TollFreeDeals.

Notifications of Fraudulent Robocall Traffic From AT&T

39. In May 2017, AT&T notified Nicholas Palumbo that it had traced back to TollFreeDeals robocalls received by AT&T customers in which the source number was spoofed to show a number belonging to USCIS; another number was spoofed to show the Office of the Inspector General of the U.S. Department of Homeland Security ("DHS-OIG"). AT&T informed Nicholas Palumbo that the callers who spoke to AT&T's customers impersonated U.S. Immigration Officers, and that AT&T had confirmed with USCIS and DHS-OIG that those agencies did not make outbound calls from either of the spoofed phone numbers. Nicholas Palumbo responded that the calls had been transmitted to TollFreeDeals from an India-based customer, and that he had blocked those two specific phone numbers. Blocking specific numbers is an ineffective means to stop fraudsters who are willing and have the ability to spoof any number for their fraud calls.

40. In February 2019, AT&T notified Nicholas Palumbo that it had traced back 19 separate calls to AT&T customers that spoofed a USCIS phone number in order to "extort money from our customers." In Nicholas Palumbo's response to AT&T, he acknowledged that those calls had been transmitted to TollFreeDeals from the same India-based VoIP carrier that had transmitted the spoofed USCIS calls in 2017. Despite repeated warnings from AT&T that this customer was transmitting fraudulent government-impersonation robocalls, the Palumbos continued transmitting VoIP calls on behalf of this customer through at least as recently as June 2019.

Records of the Calls Transmitted by TollFreeDeals are Filled with Evidence of Fraud

41. SSA obtained call detail records from TollFreeDeals for all call traffic transmitted from India-based VoIP carrier Company A to TollFreeDeals between May 6, 2019 and June 30, 2019. During that period, Company A transmitted 182,023,773 calls to phones of U.S. call recipients through TollFreeDeals. These calls came from more than ten million unique source numbers, the vast majority of which were U.S. phone numbers. Based on my training and experience, there is no legitimate business purpose for which one or several foreign call centers would use millions of different U.S. source numbers to transmit calls originating abroad. This massive volume of different source numbers, as well as the ratio of source numbers to calls, is indicative of the use of random, spoofed source numbers in order to: (1) make it appear to potential victims that the calls originate in the United States, and (2) mask from legitimate U.S. carriers and law enforcement the fact that all of these millions of fraudulent calls are originating from the same source.

42. Of these more than 182 million calls, more than 2.8 million were made to phone numbers with area codes locating them within the Eastern District of New York.

43. In the call detail records related to Company A, one thousand different unique source numbers accounted for more than 90% of the calls, more than 164 million calls. SSA OIG requested records regarding these 1,000 source numbers from YouMail, a company that provides robocall-blocking software that can be downloaded for free on any cellular phone, and which maintains detailed analytics records regarding all calls blocked on behalf of its more than 10 million subscribers. Specifically, YouMail maintains data regarding the type of scam voicemails left for its customers. Records obtained from YouMail demonstrate that 79% of the top 1,000 source numbers from the Company A call detail records have been identified as sending scam

calls. Aggregating the number of calls made by each of the source numbers identified by YouMail as sending fraudulent robocalls, Company A transmitted more than 143 million fraudulent robocalls to U.S. call recipients through TollFreeDeals between May 6, 2019 and June 30, 2019. Based on YouMail's categorization of those scam calls, almost 20% (more than 31 million calls) were SSA imposter calls, another 35% (more than 57 million calls) were loan approval scams, and 14% (more than 23 million calls) were Microsoft Refund Scams,[3] a subset of Tech Support impersonation scams.

44. The Consumer Sentinel database maintained by the FTC contained consumer complaints regarding 923 of the 1,000 source numbers from the call detail records related to Company A. As of August 2019, the Consumer Sentinel database contained 58,225 complaints regarding those 923 source phone numbers.

45. SSA OIG also obtained call detail records from TollFreeDeals regarding all VoIP call traffic terminated in the United States by TollFreeDeals on behalf of all customers between May 20, 2019 and June 11, 2019. During that 23 day time period, TollFreeDeals transmitted a total of 720,008,294 calls from its customers to U.S. call recipients. TollFreeDeals also provided records to SSA-OIG demonstrating that these roughly 720 million calls were terminated on behalf of 67 unique customers. Those calls originated from more than 133 million unique source numbers, the vast majority of which were U.S. phone numbers. Of those more than 720 million calls, more than 425 million, or 59% of the total calls, lasted less than one second in duration. SSA

[3] In a Microsoft Refund Scam, call recipients receive a message stating that a tech support company is going out of business and the recipient is entitled to a refund for services previously purchased. Once a call recipient returns the call, a fraudster in a call center convinces the recipient that the tech company's refund department inadvertently refunded the call recipient thousands of dollars, rather than hundreds of dollars. The fraudster then convinces the call recipient to wire money to return the purported refund overpayment.

OIG has learned from discussions with U.S. telecommunications carriers and with employees of USTelecom, that in the telecommunications industry, such high volumes of short-duration and unanswered calls are indicative of robocalls that are unwanted by the recipients, often because they are fraudulent. Calls from Company A accounted for roughly 11% of TollFreeDeals' total call traffic during this 23 day period.

46. Of the more than 720 million calls transmitted by TollFreeDeals during this 23 day period, 24,371,682 were made to phone numbers with area codes locating them within the Eastern District of New York. More than 14 million calls had a duration of less than one second, and more than 22 million calls had a duration of less than 30 seconds.

47. Department of Justice analysts identified the top 1,000 source numbers that sent the highest volume of calls across all TollFreeDeals customers during this 23-day period. Those top 1,000 source numbers combined sent more than 169 million calls, roughly 23.5% of all calls. SSA OIG obtained records related to these 1,000 phone numbers from YouMail and from FTC's Consumer Sentinel database. FTC received complaints regarding 460 of the top 1,000 source numbers, accounting for more than 112 million calls. YouMail records revealed that 441 of the source numbers, accounting for more than 90 million were categorized as scam calls. Based on just these top 1,000 source numbers sending the highest volume of calls, 29 unique TollFreeDeals customers transmitted call traffic from source numbers that YouMail and/or FTC records associated with fraudulent robocalls.

Defendants Provide Toll Free Numbers to Foreign Robocall Fraudsters

48. Not only do Defendants knowingly pass fraudulent robocalls by the millions into the U.S. telephone system, but they also provide return-calling services to fraudsters so that potential victims can call them back. These toll-free telephone numbers and related services are

provided in the robocall message as call-back numbers, and appear to be U.S. telephone numbers and thus enable fraudsters to further deceive individuals about the robocall's origin and the identities and locations of the fraudsters at the other end of the call. In reality, what appears to the individual to be a U.S. telephone number is just a telephone number that Defendants register to an internet address designated by the fraudsters. Thus, the toll-free numbers can be used to ring telephones anywhere in the world.

49. While toll-free numbers used for return-calling purposes cannot be "spoofed" like outgoing robocalls, the use of a U.S. toll-free number in Defendants' robocalls schemes serves much the same purpose as spoofing—deception. The toll-free services provided by Defendants use VoIP technology to direct potential victims' return calls from the United States to the foreign fraudsters' call centers. The Defendants have knowingly provided toll-free numbers and associated calling services to foreign robocall fraudsters.

50. All toll-free numbers in the United States are administered by Somos, Inc., a company designated by the Federal Communications Commission ("FCC") as the national administrator of the U.S. toll-free calling system and its database. Among other functions within the industry, Somos registers "Responsible Organizations," that are authorized to provide toll-free numbers to their customers and to register those numbers in the national registry that the industry uses to direct toll-free telephone traffic. Defendants obtain toll-free numbers on behalf of their customers from one or more responsible organizations.

51. On July 31, 2019, an employee of a Responsible Organization sent the message below to Nicholas Palumbo via his @tollfreedeals.com email address:

Hello,

We received a call yesterday (at 6 pm) that we didn't answer.

> Calling Number: +844[XXXXXXX]
> Requesting to call back: 844-[XXX]-[XXXX]
>
> Please see the attached audio and screenshot of the voicemail transcript. Shut down this user immediately as it was associated with the customer account of [TollFreeDeals customer]. These types of scam calls are prohibited from our network and further fraudulent calls from the same customer account will result in termination of said customer account. The number of 844-[XXX]-[XXXX] has been removed from your account in order to protect the integrity of our network.

I listened to the audio file, and the statement below is a true and correct transcription of the audio I heard:

> tomorrow $399.99 is going to be deducted from your account for the remainder of your computer services. If you want to cancel the subscription, please press 1 to talk to our cancellation officer. Or you can call us back on our help line number 1-844-[XXX]-[XXXX]. I'll repeat the help line number 1-844-[XXX]-[XXXX]. Thank you."

52. From August 1, 2019, through August 9, 2019, the Responsible Organization sent an additional six emails to Nicholas Palumbo, notifying him that the Responsible Organization was removing eight additional toll-free numbers from the accounts of two TollFreeDeals customers, because those numbers had been shown to be used in Tech Support impersonation scams and scams impersonating Amazon customer service. In response to each email, Nicholas Palumbo responded to the effect that he had informed his customer.

53. On August 12, 2019, an employee of the Responsible Organization emailed Nicholas Palumbo and stated:

> Good afternoon Nick,
>
> I wanted to reach out to inform you that we have disabled the account of [TollFreeDeals customer] due to fraudulent complaints. Unfortunately, we do get a lot of complaints about customers under your reseller account. Our first line of defense when issues like arise we deactivate the customer's account. I am informing you that if we do receive any additional complaints about any of your other customers under your re-seller account, we will be forced to deactivate your account.

54. That same date, Nicholas Palumbo responded "I let him know," then responded further, "I will be porting clients over[.] Can't take that chance." In the telecommunications industry, to "port a number" means to move an existing phone number from one provider to another. In effect, Nicholas Palumbo was stating that he planned to take the toll-free numbers registered to his customers through the Responsible Organization who had warned him about fraudulent calls, and move those same numbers to another provider on behalf of his customers. The August 12, 2019, email correspondence referenced in this paragraph is attached as Exhibit 2.

55. On May 11, 2019, Nicholas Palumbo emailed himself a reminder to "Order 10 toll frees" for India-based VoIP carrier Company A.

Pursuant to 28 U.S.C. § 1746, I hereby declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief. Executed on January 27th, 2020, in Scottsdale, Arizona.

Marey Ralston
Special Agent, SSA OIG

EXHIBIT 1

2019-08-14 18:16:02 UTC: Sent Formal email to nick@tollfreedeals.com

USTELECOM | THE BROADBAND ASSOCIATION

To Whom It May Concern:

By way of introduction, my name is Farhan Chughtai, and I coordinate the efforts of USTelecom's Industry Traceback Group. We are writing to request your assistance on industry efforts focused on our shared interests of protecting consumers from fraudulent, abusive or potentially unlawful robocalls. My contact information is listed below, and I would be more than happy to discuss this request with you over the phone.

A member of USTelecom's Industry Traceback Group recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin (call details with date(s) are listed below). We request that you assist industry stakeholders who are engaging in traceback efforts in order to help identify the source of this potentially fraudulent, abusive or unlawful network traffic. To assist us in our efforts, **we are asking that you respond to this traceback inquiry as soon as possible, but no later than three business days from now.**

Please note that the FCC's Enforcement Bureau recently reached out to carriers that were not supporting these traceback efforts (discussed below). In addition, USTelecom has recently initiated an automated system for conducting tracebacks. We are asking that you submit your response to this inquiry via our secure on-line portal, where you can see additional detail about all traceback requests involving your network. With respect to the call details below, can you please provide us with the following:

1. Please investigate the source of this traffic and respond with the identity of the upstream carrier(s) that sent the traffic into your network, or if one of your end users originated the traffic, please state as such and identify that end user. **We ask that you use the link below to access the portal and use the drop-down selector to provide this information.**

2. If, in investigating this traffic, the end user(s) originating the traffic are able to demonstrate to you that the traffic complies with applicable United States laws and regulations, please respond via email to me with the description of the traffic, the identity of the customer, and the customer's explanation.

3. As you investigate this matter, please take appropriate action on your network to ensure compliance with applicable United States laws and regulations, and inform me of the action you have taken.

Regarding this request, USTelecom has a group of members and non-members dedicated to tracing back fraudulent, abusive, and/or unlawful traffic to its source (called the "Trusted Carrier Framework") so that such calls never reach consumers. USTelecom is a 501(c)(3) industry trade association that is coordinating the efforts of the Trusted Carrier Framework. This cooperative framework includes a broad range of industry participants (including ILECs, CLECs, VoIP providers, long distance companies, and wholesale providers), who are working to reduce the number of robocalls consumers receive and help identify their origins. This traceback framework – and others like it – operate under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI).

We invite you to join our industry traceback efforts; there is no cost to do so. Please call or email to have your preferred contact information added to our systems.

Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." Recently the FCC's Enforcement Bureau sent a series of letters – some under its Section 403 investigation authority – to carriers that have been non-responsive to USTelecom's traceback request (see here: https://docs.fcc.gov/public/attachments/DOC-354942A2.pdf). The letters "urged" carriers to "to cooperate with the USTelecom Industry Traceback Group's program aimed at identifying the source of illegal robocalls and harmful spoofed calls."

In addition, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of USTelecom's Trusted Carrier Framework, disclosure of this information fits within that exception. To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom advises the appropriate law enforcement agencies so that they can take appropriate action against the caller, should they elect to do so. Similarly, if this industry effort fails to trace these calls their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to contact me should you have any questions, or would like to discuss.

Thanks,
Farhan

Farhan Chughtai
Director, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
https://traceback.ustelecom.org/Form/Login/r;REDACTED?t=kF9qfzR7iyG
(URL is a private login; do not share.)

Call Details for Incident #690 (new)

Date/Time:	2019-08-05 15:07:00 UTC
To:	+13013437570
From:	+18004038700
Campaign:	SSA-BenefitsCanceled
	Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated message threatens that social security benefits will be canceled. Caller-ID appears to be a random toll-free number. Called party is asked to press 1 to speak to an agent. Caller-ID is random (different on each call) so blocking the ANI is not effective.

Call Details for Incident #724 (new)

Date/Time:	2019-08-12 14:03:00 UTC
To:	+15864892755
From:	+18883716781
Campaign:	SSA-Jun2019
	Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated voice claims suspicious activity on your social security number; press 1. Calls are from apparently random 8XX numbers or other geographic numbers. Call volume estimated at over a million per day. Because Caller-ID changes with each call, blocking the ANI is not effective.

Call Details for Incident #723 (new)

Date/Time:	2019-08-12 14:10:00 UTC
To:	+12488083416
From:	+19562547097
Campaign:	SSA-Jun2019
	(see description above)

Call Details for Incident #722 (new)

Date/Time:	2019-08-12 14:40:00 UTC
To:	+12485055710
From:	+19567226365
Campaign:	SSA-Jun2019
	(see description above)

Call Details for Incident #687 (9d3h ago)

Date/Time:	2019-08-05 14:10:00 UTC
To:	+12155344889
From:	+18786525758
Campaign:	SSA-Jun2019
	(see description above)

EXHIBIT 2

On Mon, Aug 12, 2019 at 2:23 PM -0700, "JR Voltaggio" <jr@teli.net> wrote:

> Good afternoon Nick,
> I wanted to reach out to inform you that we have disabled the account of [redacted] due to fraudulent complaints. Unfortunately, we do get a lot of complaints about customers under your re-seller account. Our first line of defense when issues like arise we deactivate the customer's account. I am informing you that if we do receive any additional complaints about any of your other customers under your re-seller account, we will be forced to deactivate your account.
>
> **JR Voltaggio**
>
> Customer Success Manager
> Office (844) 411-1111
> jr@teli.net
> www.teli.net

To	JR Voltaggio <jr@teli.net>
From	nick palumbo <nick@tollfreedeals.com>
Date/Time - UTC+00:00 (M/d/yyyy)	8/12/2019 9:36:58 PM
Subject	Re: Account [redacted]
Body	I let him know

To	JR Voltaggio <jr@teli.net>
From	nick palumbo <nick@tollfreedeals.com>
Date/Time - UTC+00:00 (M/d/yyyy)	8/12/2019 9:37:15 PM
Subject	Re: Account [redacted]
Body	I will be porting clients over Can't take that chance

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

Plaintiff,

v.

NICHOLAS PALUMBO, NATASHA PALUMBO, ECOMMERCE NATIONAL, LLC d/b/a Tollfreedeals.com, and SIP RETAIL d/b/a sipretail.com,

Defendants.

CV 20 - 473
Civil Action No.

KORMAN, J.

MANN, M.J.

CERTIFICATION PURSUANT TO FED. R. CIV. P. 65(b)(1)(B)

1. I am an Assistant United States Attorney in the Civil Division at the U.S. Attorney's Office for the Eastern District of New York. I make this certification pursuant to Fed. R. Civ. P. 65(b)(1)(B) in support of the United States' application for a temporary restraining order pursuant to 18 U.S.C. § 1345, whereby defendants Nicholas Palumbo, Natasha Palumbo, Ecommerce National, LLC d/b/a Tollfreedeals.com, and SIP Retail d/b/a sipretail.com (collectively, "Defendants") would be enjoined from engaging in an ongoing wire fraud scheme in violation of 18 U.S.C. §§ 1341 and 1349.

2. As set forth in detail in the accompanying Complaint and the Declarations of Special Agent Marcy Ralston of the Social Security Administration's Office of the Inspector General, and Postal Inspector Samuel Bracken of the United States Postal Inspection Service, the Defendants are utilizing the U.S. telecommunications network to participate in an ongoing scheme to defraud through facilitating the delivery of vast numbers of fraudulent telephone calls to victims,

among other fraudulent conduct, resulting in harm to victims throughout the United States, including elderly and vulnerable victims.

3. The Ralston and Bracken Declarations, together with the Complaint and accompanying exhibits, specifically set forth facts showing that the Defendants' conduct subjects thousands of victims to immediate and irreparable financial loss or other harm. The Declarations and Complaint further establish that the frauds are ongoing, and will continue to cause harm to victims during the interval between Defendants being given further notice and the Court's ruling on the United States' application for temporary relief. The Declarations and Complaints establish that Defendants continue to transmit large volumes of fraudulent telephone calls on a regular basis.

4. The temporary restraining order sought by the United States would enjoin Defendants from: (1) committing wire fraud, as defined by 18 U.S.C. §§ 1343 and 1349; (2) providing, or causing others to provide, call termination services for calls terminating in the United States or carrying any VoIP calls terminating in the United States; (3) providing toll-free telephone services for calls originating in the United States, including providing toll-free phone numbers to other individuals or entities; and (4) destroying, deleting, removing, or transferring any and all business, financial, accounting, and other records concerning Defendants' operations and the operations of any other corporate entity owned or controlled, in whole or in part, by Defendants. The requested relief would therefore immediately prevent harm to new victims.

5. The Court should not require the United States to provide notice to the Defendants prior to the entry of the requested relief, because notice potentially could allow the Defendants to destroy relevant business records before the parties are heard by the Court. In addition, during the time it would take to give Defendants notice, additional persons could be victimized through Defendants' regular delivery of fraudulent telephone calls through U.S. telecommunications

network, Defendants' provision of toll-free calling services used to further the wire fraud schemes, and through other conduct by Defendants in furtherance of the scheme such as through Defendants' receipt of funds from defrauded victims.

6. Therefore, the United States respectfully requests that the Court issue the proposed temporary restraining order without notice to Defendants.

Dated: January 28, 2020
Brooklyn, New York

DARA A. OLDS
Assistant United States Attorney
Tel. (718) 254-6148
dara.olds@usdoj.gov

EXHIBIT 3

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

Plaintiff,

v.

JON KAHEN, a/k/a JON KAEN, GLOBAL VOICECOM, INC., GLOBAL TELECOMMUNICATION SERVICES INC., and KAT TELECOM, INC.,

Defendants.

COMPLAINT

Civil Action No.

CV 20-00474

COGAN, J.

Plaintiff, the UNITED STATES OF AMERICA, by and through the undersigned attorneys, hereby alleges as follows:

INTRODUCTION

1. The United States brings this action for a temporary restraining order, preliminary and permanent injunctions, and other equitable relief pursuant to 18 U.S.C. § 1345, in order to enjoin the ongoing commission of criminal wire fraud in violation of 18 U.S.C. § 1343 and conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349. The United States seeks to prevent continuing and substantial injury to the victims of fraud.

2. Since at least 2017 and continuing through the present, Defendant John Kahen, a/k/a Jon Kaen ("Kaen"), together with one or more co-conspirators, has used the U.S. telephone system to engage in predatory wire fraud schemes that victimize individuals throughout the United States, including individuals within the Eastern District of New York and significant numbers of elderly and vulnerable victims. Kaen controls various corporate entities that he utilizes in furtherance of the fraudulent scheme, including Defendants Global Voicecom, Inc.; Global

Telecommunications Services Inc.; and KAT Telecom, Inc. (the "Corporate Defendants," and together with Kaen, the "Defendants). The Corporate Defendants, based in New York, are VoIP[1] carriers that serve as "gateway carriers"[2] facilitate the delivery of millions of fraudulent "robocalls"[3] every day from foreign call centers and foreign VoIP carriers to the U.S. telecommunications system and ultimately to phones throughout the United States. The Defendants thus provide foreign fraudsters the means to access the U.S. telephone system, knowingly passing millions of fraudulent robocalls intended to deceive the recipient into: (1) answering or returning the call, and (2) paying money to the perpetrators of the schemes.

3. Through these robocalls, fraudsters operating overseas impersonate government entities and well-known businesses by "spoofing"[4] legitimate phone numbers and sending recorded messages that are transmitted across the internet to telephones throughout the United States. These robocalls purport to be from federal government agencies, elements of foreign governments, and legitimate businesses, conveying alarming messages, such as that the call recipient's social security number or other personal information has been compromised or otherwise connected to criminal activity; the recipient faces imminent arrest; the recipient's assets are being frozen; the recipient's bank and credit accounts have suspect activity; the recipient's

---

[1] VoIP stands for voice-over-internet protocol and allows users to place phone calls over a broadband internet connection.

[2] As set forth in further detail herein, "gateway" carriers are the first in a chain of VoIP carriers located in the United States that facilitate the delivery of foreign VoIP calls to receipients in the United States.

[3] "Robocall" means a call made through an automated process that places large volumes of telephone calls over the internet in order to deliver recorded messages, in contrast to calls placed one at a time by a live person.

[4] The practice of making a false number appear on the recipient's caller ID is known as "spoofing."

benefits are being stopped; the recipient faces imminent deportation; or combinations of these things—all lies intended to induce potential victims to speak to the fraudsters. When individuals answer the calls or return voicemail messages, the fraudsters offer to "resolve" these legal matters by immediate transfers of funds to settle the purported legal obligation, or to hold the individual's assets only temporarily while the crisis resolves. In reality, the individual is neither under investigation nor in legal jeopardy, and the same threatening robocall was made simultaneously to thousands of other U.S. telephones.

4. Not only do Defendants deliver vast numbers of fraudulent robocalls every day, but they also participate in the fraudulent schemes by providing return-calling services to the fraudsters used to establish contact with potential victims. Robocall messages will often provide domestic and toll-free call-back numbers; potential victims who call these numbers connect to the overseas fraudsters, who then try to extort and defraud the potential victims.

5. The Defendants profit from these fraudulent robocall schemes by receiving payment from their co-conspirators for the services Defendants provide. In addition, on at least one occasion Defendants received a direct payment from a victim of one of the fraudulent schemes.

6. Since 2017 and continuing through the present, as a result of their conduct, Defendants and their co-conspirators have defrauded numerous victims out of millions of dollars, including victims in the Eastern District of New York.

7. For the reasons stated herein, the United States requests injunctive relief pursuant to 18 U.S.C. § 1345 to enjoin Defendants' ongoing scheme to commit wire fraud in violation of 18 U.S.C. § 1343 and conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349.[5]

[5] This case is one of two cases being filed simultaneously in which the United States Department of Justice, for the first time, seeks to enjoin telecommunications companies from participating in robocalling fraud schemes pursuant to 18 U.S.C. § 1345.

JURISDICTION AND VENUE

8. The Court has subject matter jurisdiction over this action pursuant to 18 U.S.C. § 1345 and 28 U.S.C. §§ 1331 and 1345.

9. Venue lies in this district pursuant to 28 U.S.C. § 1391(b)(2).

PARTIES

10. Plaintiff is the United States of America.

11. Defendant Kaen resides in Nassau County, New York, in the Eastern District of New York. Kaen controls Defendants Global Voicecom, Inc., Global Telecommunication Services Inc., and KAT Telecom, Inc., which he uses in furtherance of the fraudulent robocall scheme. Kaen operates the Corporate Defendants as a single enterprise from his home in the Eastern District of New York. One or more of the Defendants also conducts business as "IP Dish."

12. Defendant Global Voicecom, Inc. is a New York corporation. The New York Department of State, Division of Corporations Entity Information database identifies Global Voicecom's principal executive office as being located in Great Neck, New York, in the Eastern District of New York, and Kaen as the corporation's Chief Executive Officer.

13. Defendant Global Telecommunication Services Inc. is a New York corporation. Global Telecommunication Service's principal place of business is located in Great Neck, New York, in the Eastern District of New York.

14. Defendant KAT Telecom, Inc. is a New York corporation. KAT Telecom's principal place of business is located in Great Neck, New York, within the Eastern District of New York.

OVERVIEW OF THE ROBOCALLING FRAUD SCHEMES

A. Robocalling Fraud Targeting Individuals in the United States

15. The robocalling fraud schemes in which the Defendants are engaged share the same characteristics. Individuals at call centers located abroad, many of which are operating out of India, are bombarding the U.S. telephone system every day with millions of robocalls intended to defraud individuals in the United States. Many of these fraudsters impersonate U.S. government officials, foreign government officials, or well-known American businesses, in order to threaten, defraud, and extort money from robocall recipients. Robocalling technology, which allows fraudsters to send millions of calls per day all transmitting the same pre-recorded, fraudulent message, enables fraudsters to cast a wide net for elderly and vulnerable victims who are particularly susceptible to the threatening messages the fraudsters are sending. Even if only a small percentage of the recipients of a fraudulent call center's robocalls connect with potential victims, the fraudsters can still reap huge profits from their schemes.

16. Foreign fraudsters operate many different schemes targeting individuals in the United States, but the Defendants' robocall schemes include the following categories of impersonation scams:

a. *Social Security Administration ("SSA") Imposters*: Defendants transmit recorded messages in which SSA imposters falsely claim that the call recipient's social security number has been used in criminal activity, the individual's Social Security benefits will be suspended, the individual has failed to appear before a grand jury and face imminent arrest, or the individiual's social security number will be terminated. When a call recipient calls back or connects to the fraudster, the fraudster claims to be an SSA employee and typically tells the individual to transfer substantial funds to the SSA for safekeeping until a new social security number can be issued, at which point the individual's funds purportedly will be returned.

b. *Internal Revenue Service ("IRS") and Treasury Imposters*: Defendants transmit recorded messages in which IRS imposters falsely claim that the call recipient has been implicated in tax fraud, the individual has avoided attempts to enforce criminal laws, the individual has avoided court appearances, or the individual faces imminent arrest. When a recipient calls back or connects to the fraudster, the fraudster claims to be an IRS or Treasury employee and typically tells the recipient to transfer funds to the IRS to resolve various fictitious tax and legal liabilities, or for safekeeping in order to avoid seizure of assets.

c. *United States Citizenship and Immigration Services ("USCIS") Imposters*: Defendants transmit recorded messages in which USCIS imposters falsely claim that the call recipient has failed to fill out immigration forms correctly, the individual faces imminent arrest or deportation, that the individual's home country has taken formal action that may result in deportation, or the individual has transferred money in a way that will result in deportation. When a call recipient calls back or connects to the fraudster, the fraudster claims to be a USCIS employee and typically tells the individual to pay various fees or fines to avoid immigration consequences.

d. *Foreign Government Imposters*: Defendants transmit recorded messages in which foreign government imposters, often in foreign languages, falsely claim to be from the U.S.-based consulate of a foreign government and that the call recipient faces problems with immigration status or a passport. When a call recipient calls back or connects to the fraudster, the fraudster falsely claims that the individual must

pay various fees or fines in order to avoid immigration consequences such as deportation.

e. *Tech Support Imposters*: Defendants transmit recorded messages in which fraudsters operating tech support scams impersonate various well-known tech companies such as Apple or Microsoft, and falsely claim that the call recipient has computer security problems that require assistance. When an individual connects with the fraudster, the fraudster instructs the individual to pay for fictitious tech support and computer security services, and to allow the fraudster remote access to the victim's bank accounts.

17. These robocalls are often "spoofed" so that they falsely appear on a victim's caller ID to originate from U.S. federal government agency phone numbers, such as the SSA's main customer service number, from local police departments, 911, or from the actual customer service phone numbers of legitimate U.S. businesses. These "spoofed" numbers are used to disguise the origin of the robocalls and the callers' identities, and to cloak them with the authority of government agencies or large businesses to induce potential victims to answer or return the calls. In reality, the calls originate from fraudsters operating abroad, and have no connection to any U.S. government agency or other legitimate enterprise.

18. Individuals who answer or otherwise respond to these calls eventually speak to live fraudsters who tell the individuals lies intended to frighten and confuse them so that the fraudsters may begin to control their behavior and isolate them from authorities, friends, and family members. These lies often include that the individual's social security number or other personal information has been implicated in criminal activity, that the individual faces imminent arrest or deportation, and that the individual's assets are about to be forfeited to the government. Once an individual is

overcome by fear and panic, the fraudsters keep them on the phone and offer reassurances that the individual's purported legal problems can be resolved through payment of money, or that the individual's money must be transferred for safekeeping to the government agency the fraudsters are impersonating. The fraudsters often claim that the victim's payment will be returned to them in the immediate future. In reality, once the fraudsters are convinced they have extorted as much money as possible from the victim, they drop all contact, leaving the victim without meaningful recourse. Fraudsters receive victims' money through retail gift cards, bank wires, cash payments, cryptocurrency transfers, and other methods.

19. Since October 2018, the most prolific robocalling scam impersonating U.S. government officials—and one engaged in by Defendants—is impersonation of the SSA. For example, a robocall sent to millions of phones in the United States in early 2019 contained the following message:

> Hello this call is from Department of Social Security Administration the reason you have received this phone call from our department is to inform you that there is a legal enforcement actions filed on your social security number for fraudulent activities so when you get this message kindly call back at the earliest possible on our number before we begin with the legal proceedings that is 619-[XXX]-[XXXX] I repeat 619-[XXX]-[XXXX] thank you.

20. SSA received more than 465,000 complaints about fraudulent telephone impersonation of the Administration from October 1, 2018 through September 30, 2019. Losses associated with these complaints exceed $14 million. Similarly, the Federal Trade Commission ("FTC") reported that for 2018, its Consumer Sentinel database received more than 39,000 fraud complaints about SSA imposter calls, with estimated losses of approximately $11.5 million; for 2019, the FTC reported that SSA imposter call complaints rose to approximately 166,000 with

associated losses of more than $37 million.[6] Complaint numbers substantially underrepresent the extent of the problem, because most victims do not report their losses to the government.

B. How Calls From Foreign Fraudsters Reach U.S. Telephones

21. The Defendants' robocalling fraud schemes, which involve robocalls that originate abroad and target individuals in the United States, are all dependent on VoIP and related technology to create the calls. VoIP calls use a broadband internet connection—as opposed to an analog phone line—to place telephone calls locally, long distance, and internationally, without regard to whether the call recipient uses a cellular phone or a traditional, wired phone. The robocalling fraud schemes also require U.S.-based telecommunications companies—referred to as "gateway carriers"—to introduce the foreign phone traffic into the U.S. phone system. A foreign call center or telecommunications company that places VoIP calls to U.S. telephones must have a relationship with a U.S. gateway carrier. From the gateway carrier, most VoIP calls will pass through a series of U.S.-based VoIP carriers before reaching a consumer-facing "common carrier" such as AT&T or Verizon, and ultimately a potential victim's phone. One of the Defendants' roles in the fraudulent schemes is to serve as a gateway carrier for the fraudulent robocalls.

22. Each provider in the chain that transmits a VoIP call maintains records, primarily for billing reasons, of all of the calls that pass through it. These records include the following information: the date and time of the call, the destination number (intended recipient), the source number from which the call was placed (sometimes a real number and sometimes a spoofed number), the name of the company that sent the call to the provider, and the downstream company to which the provider sent the call. These records are generated automatically as a call is routed

[6] Regarding government imposter fraud more broadly and not limited just to SSA imposters, the FTC's Consumer Sentinel database contains 255,223 complaints reflecting $128,479,054 in losses for 2018, and 389,563 complaints reflecting $152,946,623 in losses for 2019.

through telecommunications infrastructure in a manner that achieves the lowest cost to transmit a given call, known in the industry as "least-cost routing." Calls may be traced through these records back to their gateway carrier, and thus to their foreign source. The telecommunications industry refers to this tracing process as "traceback."

23. Tracebacks of many different robocalling fraud schemes have led to the identification of Defendants as a gateway carrier willing to transmit huge volumes of fraudulent robocalls into the country, despite clear indicia of fraud in the call traffic and actual notice of fraud.

DEFENDANTS' ONGOING PARTICIPATION IN ROBOCALLING FRAUD SCHEMES

24. Since at least 2017, the Defendants have knowingly provided U.S.-bound calling services to foreign fraudsters operating robocall scams, acting as a gateway carrier and passing robocalls into the U.S. telephone system by the millions. The Defendants are paid for each call they pass into and through the U.S. telephone system. In addition, the Defendants have provided return-calling services to the fraudsters operating the robocall scams, for which Defendants are also paid, enabling the fraudsters to establish contact with unwitting individuals after the individuals are deceived by a robocall.

25. There is substantial evidence of the Defendants' knowledge of the fraudulent nature of the calls they transmit, including call records showing high percentages of short-duration, unanswered calls[7] passing through their systems by the millions; thousands of spoofed calls purporting to be from "911" and similar numbers originating from overseas; dozens of complaints, warnings, and inquiries from vendors and other telecommunications companies about fraud, spoofing, and short-duration "junk" calls; repeated warnings and inquiries from an industry trade

[7] Short-duration and unanswered calls include calls where recipients immediately hang up and calls that do not connect because robocalls are sent to numerous telephone numbers that are not in service.

group about the scam robocalls passing through the Defendants' system; and receipt of numerous complaints from common-carrier telecommunications companies whose customers were victims of these fraud schemes.

A. Defendants Knowingly Introduce Fraudulent Robocalls into the U.S. Telephone System

26. In the telecommunications industry, high volumes of short-duration and unanswered calls are indicative of robocalls that are unwanted by the recipients, often because they are fraudulent. Defendants regularly transmit massive volumes of such calls. For example, the Government's investigation has revealed a sample of more than 7.7 million calls that Defendant Global Voicecom routed through a single downstream VoIP carrier over 19 days in May and June 2019, months after Kaen's response to the FCC. Of those calls, approximately 86%, more than 6.6 million calls, were one second or less in duration, indicating exceedingly high levels of junk and fraudulent robocalls. Moreover, a small sample of approximately 330,000 of these calls was examined in greater detail; of these approximately 330,000 calls in that 19-day period, more than 270,000 (approximately 81%) were from source numbers (the numbers appearing on the recipients' caller IDs) identified as fraudulent robocalls. Similarly, of the more than 106,000 robocalls spoofing the SSA's toll-free customer service number in January and February 2019 that Defendant Global Voicecom transmitted into the United States, nearly 60% had a call duration of less than one second, and another 38% were between one and 60 seconds in duration. During that same period in January and February 2019, Defendant Global Voicecom also ran through its systems thousands of calls spoofing 911, 1911, and 11911, with similar short call durations.

27. Since 2017, significant numbers of fraudulent robocalls have been traced back to the Defendants and brought to their attention. For example, U.S. common carrier AT&T has

notified Defendants on numerous occasions about fraud traced back to Defendants' operations. These notices include a November 16, 2017, email to IP Dish:

> The following calls to AT&T cell phone customers were received using the spoofed caller ID numbers of a non-working number at the US Department of Homeland Security headquarters. Callers impersonated US Citizenship and Immigration[ ] Services personnel and defrauded an AT&T customer of $1,450. . . .
> Pursuant to the customer and carrier network fraud protection provisions of the Telecommunication Act and the Telephone Records Privacy Protection Act (47 USC 222(d)(2)), could you provide the name(s) of your upstream carriers? We are tracing these calls to their source so they can be stopped.

AT&T sent similar emails about USCIS impersonation scams to Defendants Kaen and Global Voicecom in September 2017, November 2017, April 2018, and July 2018. Similarly, AT&T emailed Defendants about SSA and other imposter robocalls on January 29, 2019:

> We have been receiving AT&T customers complaints about spoofing fraud from your network. In the first complaint calls are originating from a toll free number owned by the US Social Security Administration. Callers falsely claim to be US Government officials and attempt to extort money from our customers. We have verified this number is not out-pulsed as a legitimate caller ID by the real US Social Security Administration. . . .
>
> In the second complaint calls are originating from the toll free number of DirecTV (AT&T). Callers falsely claim to be AT&T/DirecTV technical reps and social engineer remote access to our customer's computers in order to make fraudulent wire transfers from online banking applications. . . .
> Could you provide the names and contact numbers of the parties that sent these calls to your network.

AT&T sent similar warning notices about SSA imposter calls to Defendants Kaen and Global Voicecom in February 2019 and May 2019.

28. Another VoIP carrier that received call traffic from Defendants, Peerless Network, Inc., sent even more warning notices and inquiries to Defendants. For example, Peerless Network sent a warning notice about spoofed calls in September 2018 with a request that Defendants investigate and "take the appropriate action." Peerless Network sent approximately 12 of these warning notices between September 2018 and March 2019.

29. Not only have other telecommunications companies provided warnings and notices to Defendants as a result of tracebacks, but a leading industry trade group, USTelecom, has done the same. For example, USTelecom traced back an August 19, 2019 robocall that originated from India and came through Defendant Global Voicecom as the gateway carrier. The robocall was also routed through Defendant KAT Telecom. This robocall stated that there was "suspicious activity" associated with the individual's social security number. USTelecom provided the following warning notice in its correspondence to Defendant Global Voicecom on August 27, 2019:

> Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated voice claims suspicious activity on your social security number; press 1. Calls are from apparently random 8XX numbers or other geographic numbers. Call volume estimated at over a million per day. Because Caller-ID changes with each call, blocking the ANI[8] is not effective.

Blocking specific telephone numbers is an ineffective means to stop fraudsters who are willing—and have the ready ability—to spoof any number as the caller ID number for their fraudulent robocalls. For example, in January and February 2019, Defendants transmitted fraudulent robocalls spoofing 911, 1911, and 11911. Nevertheless, if the Defendants responded at all to these notices and warnings from other telecommunications–industry actors, they routinely responded that the "offending" number had been blocked, as though the spoofed telephone number and not the caller were responsible for the fraud.

30. Similarly, USTelecom traced an October 3, 2019 robocall to Defendant Global Voicecom as the gateway carrier. This robocall also originated from India. USTelecom provided

[8] "ANI" means "Automatic Number Identification," and for these purposes refers to the purported source number for the call.

the following warning notice in its October 11, 2019 correspondence to Defendant Global Voicecom:

> Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Calls placed from specific numbers obtained by scammers, using an automated voice to inform called party that they are in trouble with IRS and will be arrested. Called party is instructed to call back to speak to an agent. . . We are using traceback to try to find the source(s) of the millions of outbound calls that are being made to initiate the scam.

USTelecom's records indicate that this robocall was transcribed in part as follows:

> This call is from Federal Tax and audit division of internal revenue services. This message is intended to contact you regarding an enforcement action executed by the US treasury intending your serious attention. Ignoring this will be an intentional second attempt to avoid initial appearance before a magistrate judge or a grand jury for federal criminal offense. This is a final attempt to reach you to resolve this issue immediately and to speak to a federal agent to call us back on 510-[XXX]-[XXXX]. I repeat 510-[XXX]-[XXXX].

USTelecom identified Defendants as the gateway carrier for foreign fraudulent robocalls on at least eighteen other occasions in the latter half of 2019 alone, each time providing similar warning notices about the nature of the scam robocalls. USTelecom's records indicate that on nearly all of these 2019 tracebacks, the scam robocalls came from the same company in India.

31. Defendants transmitted another group of fraudulent robocalls that spoofed the phone number for a foreign government consulate in New York, New York. These calls conveyed foreign-language messages about problems with the individual's immigration status or passport. Like with SSA imposter robocalls and other U.S. government-imposter scams, individuals who returned the calls to the consulate imposters were told lies intended to frighten them and make them think there are imminent consequences for involvement in criminal activity, and that funds must be transferred to the fraudsters to resolve the matters. Like with the SSA imposter scams, once the fraudsters are convinced they have extorted as much money as possible, they drop all contact with the victim. In 2018, the FCC traced this consulate imposter scam back to Kaen and

IP Dish, who informed the FCC that the calls came from a Hong Kong entity that was making tens of thousands of calls per day. The FTC's Consumer Sentinel database reflects more than 1,000 complaints related to the spoofed phone number of the consulate. These complaints relate hundreds of thousands of dollars in victim losses. Defendants continue to conduct business with this Hong Kong entity more than a year later.

32. Despite these notices and numerous others, Defendants continue to pass fraudulent robocalls into the U.S. telephone system to millions of U.S. telephones every day.

B. Defendants Provide Return-Calling and Toll-Free Services for Robocall Schemes

33. Not only do Defendants knowingly pass fraudulent robocalls by the millions into the U.S. telephone system, but they also provide return-calling services to fraudsters so that potential victims can call them back. These toll-free and direct-inward-dial ("DID") telephone numbers[9] and related services are provided in the robocall message as call-back numbers, and appear to be U.S. telephone numbers and thus enable fraudsters to further deceive individuals about the robocall's origin and the identities and locations of the fraudsters at the other end of the call. In reality, what appears to the individual to be a U.S. telephone number is actually a telephone number that Defendants register to an internet address designated by the foreign fraudsters. Thus, the DID and toll-free numbers can be used to ring telephones anywhere in the world.

34. While DID and toll-free numbers used for return-calling purposes cannot be "spoofed" like outgoing robocalls, the use of a U.S. DID or toll-free number in Defendants' robocalls schemes serves much the same purpose as spoofing—deception. The DID and toll-free services provided by Defendants use VoIP technology to direct potential victims' return calls from

[9] As applicable to the fraud schemes, direct-inward-dial numbers are phone numbers with U.S. area codes that are routed to fraudulent call centers in foreign countries through VoIP technology.

the United States to the foreign fraudsters' call centers. The Defendants have knowingly provided hundreds of these DID and toll-free numbers and associated calling services to foreign robocall fraudsters.

1. DID Numbers Used to Further Robocalling Fraud Schemes

35. Like telephone numbers used to make U.S.-bound robocalls, DID numbers can be traced to identify their providers and users. This process was used to identify DID numbers provided by the Defendants for use in the fraudulent robocall schemes. For example, records obtained from one U.S. company demonstrate that it assigned 902 DID telephone numbers to Defendant Global Voicecom. Approximately 55% of these DID telephone numbers are associated with more than 28,000 complaints in the FTC's Consumer Sentinel database. One of the 902 DID telephone numbers appeared in a robocall sent to millions of U.S. telephones in early 2019:

> Hello this call is from Department of Social Security Administration the reason you have received this phone call from our department is to inform you that there is a legal enforcement actions filed on your social security number for fraudulent activities so when you get this message kindly call back at the earliest possible on our number before we begin with the legal proceedings that is 619-[XXX]-[XXXX] I repeat 619-[XXX]-[XXXX] thank you.

At the time of the robocalls, this DID telephone number was assigned to Defendant Global Voicecom, which used that DID telephone number to provide return-calling services to the overseas fraudsters. Individuals who return calls like these put themselves in a pool of likely victims, insofar as the individuals self-select through belief that the message was sufficiently credible to warrant a return call. Upon returning the call to 619-[XXX]-[XXXX], individuals were told that they were speaking to SSA agents, who offered to resolve the purported problems that prompted the call by way of immediate payment of funds. In reality, the person speaking to the individual was a fraudster, unaffiliated with the U.S. government.

36. Beginning as early as September 2017 and continuing through the present, the U.S. company that assigned these 902 DID numbers to Defendants provided numerous warning notices about how the numbers were being used to perpetrate fraud. For example, that company provided the following warning notice to Defendant Global Voicecom on September 13, 2017 and included the substance of several complaints about fraud:

> The DID: 847[XXXXXXX] which we show assigned to you, is being used for fraudulent purposes. The US Treasury Department has provided us with a few complaints which are listed below. Because of the nature of the complaints, we have disabled this number on our network.
>
> I received a call from 484-[XXX]-[XXXX] claiming that I was a subject of Treasury Fraud. [T]hey said to call back at 847-[XXX]-[XXXX]. The call was received on Friday September 8th at 4 pm. I live in Philadelphia, in the EST zone. They claimed I would be sued if I did not call back.
>
> I received a voicemail message with an automated recording claiming to be from the US Dept. of Treasury regarding tax fraud in my name. The call back number was 847-[XXX]-[XXXX]. No one answered the return call. I recently submitted via mail my 3rd installment of 2017 taxes, so I hope nothing has gone wrong in the process of receiving my payment. Is this a known scam number? Thank you.
>
> The voice message states (Pre-recorded): "Treasury my badge number is 4874. The nature and purpose of this call is regarding an enforcement action which has been executed by the [U.S.] treasury department regarding tax fraud against your name. Ignoring this would be an intentional attempt to avoid initial appearance before the majesty does or exempt or enforce criminal offence. Before this matter goes to federal claim, court house, or before you get arrested. Kindly call us back as soon as possible. The number to reach us is 847-[XXX]-[XXXX], let me repeat the number 847-[XXX]-[XXXX]. Hope to hear from you soon before the charges are pressed against you. Thank you."

Through the course of the ensuing years, Defendants continued to receive numerous similar warning notices about DID numbers and related services they provide. Defendants effectively ignored the warnings and never terminated the fraudsters' access to DID numbers for return calls.

37. In the course of the Government's investigation, SSA OIG agents obtained from Global Voicecom call records for seven of the 902 DID numbers assigned to Defendant Global

Voicecom that are associated with SSA imposter robocalls. According to Defendants' own records, Defendants provided these seven DID numbers to the same Indian entity that Defendant Global Voicecom identified to USTelecom as the gateway carrier for numerous government imposter scam robocalls.

38. These DID call records reveal that more than 10 million calls were placed in 2019 from more than 4.5 million unique phone numbers to the 902 DID numbers assigned to Defendant Global Voicecom. More than 240,000 of these calls were from area codes for the Eastern District of New York.

2. Toll-Free Numbers Used to Further Robocalling Fraud Schemes

39. Records from the FTC demonstrate that Defendants Global Voicecom and Jon Kaen are associated with more than 1000 October 2019 SSA-imposter robocalls to the FTC's offices. These robocalls appeared to originate from a toll-free telephone number. Toll-free numbers work in a manner similar to DID numbers, but are structured differently by the FCC and telecommunications industry. Somos, Inc. is the FCC-designated national administrator of the U.S. toll-free calling system. Among other functions within the industry, Somos registers "responsible organizations" that are authorized to provide toll-free numbers to their customers and to register those numbers in the national registry that the industry uses to direct toll-free telephone traffic. On October 23 and 24, 2019, the FTC's offices received approximately 1,000 robocalls with the following recording:

> …social security on an immediate basis as your social has been found some suspicious for committing fraudulent activities across the United State. Before we go ahead and suspend your social security permanently, we want you to call us back on our department toll free number at 877-[XXX]-[XXXX]. I repeat 8-877-[XXX]-[XXXX]. Do not disregard this message, and call us back as soon as possible. Thank you.

The toll-free 877 number appeared on the FTC's caller ID as well as in the actual robocall message as the return-call number. On October 24, 2019, an FTC investigator contacted Somos to determine which responsible organization was associated with that toll-free number, which Somos duly provided. The FTC investigator then contacted that responsible organization, who informed the investigator that the number was assigned to Defendants Global Voicecom and Jon Kaen.

40. That responsible organization provided numerous notices to Defendants concerning the toll-free numbers assigned to Global Voicecom and how they were being used to facilitate robocalling fraud, doing so 37 times between March 2019 and October 2019. For example, on April 8, 2019, the responsible organization emailed Defendant Global Voicecom: "We received a scam complaint on the number 888-[XXX]-[XXXX] and were asked to disconnect it. We dialed this number and found it was someone impersonating Microsoft, and is still connected." Similarly, on June 11, 2019, the responsible organization emailed Defendant Global Voicecom: "Please know that we have rec[ei]ved a serious complaint on TFN 888-[XXX]-[XXXX], which we see i[s] assigned to your account. This number was reported as a part of an "Amazon Customer Support Scam." On August 26, 2019, the responsible organization emailed Defendant Global Voicecom: "Please note that we have received reports that 877-[XXX]-[XXXX] is being used to spoof Bank of America. Can you please look into this, inform us of your results and take action if necessary?" To each of the dozens of notices, Defendants responded to the effect that the "offending" number has been blocked, as if the spoofed telephone number and not the caller were committing fraud, but never that they terminated the sources of the fraudulent robocalls.

41. The FTC's Consumer Sentinel reflects more than 1,400 complaints associated with the toll-free numbers assigned to Defendant Global Voicecom.

HARM TO VICTIMS

42. Defendants' fraudulent schemes have caused substantial harm to numerous victims, including many victims located in the Eastern District of New York. It is estimated that Defendants and their foreign co-conspirators defrauded victims out of millions of dollars per year through fraudulent robocalls and return-calling services. If allowed to continue, these losses will continue to rise and result in further harm to victims.

43. In addition to the massive cumulative effect of these fraud schemes on U.S. victims, the harm can be devastating to individual victims. Victims have faced terrifying threats from fraudsters impersonating government officials and have lost substantial sums of money.

44. Defendants' fraudulent schemes are ongoing and wide-ranging. Absent injunctive relief by this Court, the Defendants will continue to cause injury to victims in this District and throughout the United States, and the victims' losses will continue to mount.

COUNT I

(18 U.S.C. § 1345 – Injunctive Relief)

45. The United States realleges and incorporates by reference paragraphs 1 through 44 of this Complaint as though fully set forth herein.

46. By reason of the conduct described herein, Defendants violated, are violating, and are about to violate 18 U.S.C. §§ 1343 and 1349 by executing or conspiring to execute schemes or artifices to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises with the intent to defraud, and in so doing, transmitting or causing to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, writings, signs, signals, pictures, or sounds for the purpose of executing such schemes or artifices.

47. Upon a showing that Defendants are committing or about to commit wire fraud, conspiracy to commit wire fraud, or both, the United States is entitled, under 18 U.S.C. § 1345, to a temporary restraining order, a preliminary injunction, and a permanent injunction restraining all future fraudulent conduct and any other action that this Court deems just in order to prevent a continuing and substantial injury to the victims of fraud.

48. As a result of the foregoing, Defendants' conduct should be enjoined pursuant to 18 U.S.C. § 1345.

PRAYER FOR RELIEF

WHEREFORE, the plaintiff United States of America requests of the Court the following relief:

A. That the Court issue an order, pursuant to 18 U.S.C. § 1345, pending a hearing and determination on the United States' application for a preliminary injunction, that Defendants, their agents, officers and employees, and all other persons and entities in active concert or participation with them are temporarily restrained from:

i. committing and conspiring to commit wire fraud, as defined by 18 U.S.C. §§ 1343 and 1349;

ii. providing, or causing others to provide call termination services for calls terminating in the United States or carrying any VoIP calls terminating in the United States;

iii. providing direct-inward-dial or toll-free telephone services for calls originating in the United States, including providing direct-inward-dial or toll-free phone numbers to other individuals or entities;

iv. destroying, deleting, removing, or transferring any and all business, financial, accounting, call detail, and other records concerning Defendants' operations and

the operations of any other corporate entity owned or controlled, in whole or in part, by Defendants;

B. That the Court further order, pursuant to 18 U.S.C. § 1345, that within two days from Defendants' receipt of this Temporary Restraining Order and Order to Show Cause, Defendants shall provide copies of this Temporary Restraining Order and Order to Show Cause to all of their customers for whom they provide (1) United States call termination services, (2) United States direct-inward-dial services, or (3) United States toll-free call origination services; and to all entities (a) with whom Defendants have a contractual relationship for automated or least-cost call routing, or (b) from whom Defendants acquire direct-inward-dial numbers or toll-free numbers. Within four days from Defendants' receipt of the Temporary Restraining Order and Order to Show Cause, Defendants shall provide proof of such notice to the Court and the United States, including the names and addresses or email addresses of the entities and/or individuals to whom the notice was sent, how the notice was sent, and when the notice was sent.

C. That the Court further order, pursuant to 18 U.S.C. § 1345, Somos, Inc., in its capacity as the entity designated by the Federal Communications Commission to administer the U.S. toll-free calling system and its database, to temporarily suspend all toll-free numbers registered by or on behalf of any Defendant in this matter, until further order of this Court.

D. That the Court further order, pursuant to 18 U.S.C. § 1345, that any Toll-Free Service Provider that receives notice of this Temporary Restraining Order and Order to Show Cause and has a contractual relationship with one of the Defendants in this matter to

provide toll-free numbers, shall provide to Somos, Inc. a list of all toll-free numbers provided to that Defendant that are currently active.

E. That the Court further order, pursuant to 18 U.S.C. § 1345, that any individual or entity who has obtained a toll-free number through one of the Defendants in this matter, either directly or through another intermediate entity, and wishes to continue using that toll-free number may submit a request to the Court, copying counsel for the United States, and identifying: (1) the individual or entity's name, address, phone number, email address, website URL, and the nature of their business; (2) the end-user of the toll-free number's name, address, phone number, email address, and website URL if the end-user did not obtain the toll-free number directly from Defendants; (3) the nature of the end-user's business; (4) the purpose for which the end-user utilizes the toll-free number; (5) the date on which the individual or entity obtained the toll-free number and, if applicable, provided it to the end-user; and (6) whether the toll-free number is used by the individual, entity, or end-user in connection with robocalls. The United States shall then notify the Court within four business days whether the United States has any objection to removing the specifically identified toll-free number from the list of suspended numbers.

F. That the Court issue a preliminary injunction on the same basis and to the same effect.

G. That the Court issue a permanent injunction on the same basis and to the same effect.

H. That the Court order such other and further relief as the Court shall deem just and proper.

Dated: January 28, 2020
Brooklyn, New York

Respectfully submitted,

RICHARD P. DONOGHUE
United States Attorney

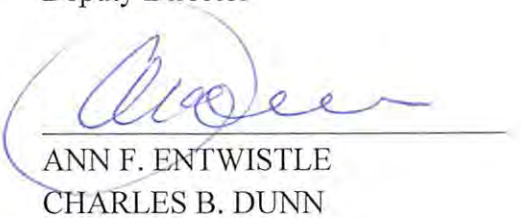
EVAN P. LESTELLE
BONNI J. PERLIN
Assistant United States Attorneys
United States Attorney's Office
Eastern District of New York
271-A Cadman Plaza East
Brooklyn, New York 11201
Tel: (718) 254-7000
Fax: (718) 254-6081
Evan.Lestelle@usdoj.gov
Bonni.Perlin@usdoj.gov

JOSEPH H. HUNT
Assistant Attorney General

DAVID M. MORRELL
Deputy Assistant Attorney General

GUSTAV W. EYLER
Director
Consumer Protection Branch

JILL P. FURMAN
Deputy Director



ANN F. ENTWISTLE
CHARLES B. DUNN
Trial Attorneys
U.S. Department of Justice
P.O. Box 386
Washington, D.C. 20044
Tel. (202) 307-0066
Tel. (202) 305-7227
Fax: (202) 514-88742
Ann.F.Entwistle@usdoj.gov
Charles.B.Dunn@usdoj.gov

CV 20 - 00510

JS 44 (Rev. 02/19)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

COGAN, J.

UNITED STATES OF AMERICA

(b) County of Residence of First Listed Plaintiff _____
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Evan P. Lestelle, Bonni Perlin
U.S. Attorney's Office, Eastern District of New York
271-A Cadman Plaza East, 7th Fl., Brooklyn, NY 11201; (718) 254-7000

DEFENDANTS

JON KAHEN, a/k/a JON KAEN, GLOBAL VOICECOM, INC., GLOBAL TELECOMMUNICATION SERVICES INC., and KAT TELECOM, INC.

County of Residence of First Listed Defendant Nassau
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☒ 1 U.S. Government Plaintiff
- ☐ 2 U.S. Government Defendant
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☒ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
Request for relief pursuant to 18 U.S.C § 1345

Brief description of cause:
Violations of wire fraud statutes, 18 U.S.C. §§ 1343, 1349

VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☐ Yes ☒ No

VIII. RELATED CASE(S) IF ANY *(See instructions)*:

JUDGE _____ DOCKET NUMBER _____

DATE 1-28-2020

SIGNATURE OF ATTORNEY OF RECORD Evan P. Lestelle

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

MJ S.J.B.

CERTIFICATION OF ARBITRATION ELIGIBILITY

Local Arbitration Rule 83.7 provides that with certain exceptions, actions seeking money damages only in an amount not in excess of $150,000, exclusive of interest and costs, are eligible for compulsory arbitration. The amount of damages is presumed to be below the threshold amount unless a certification to the contrary is filed.

Case is Eligible for Arbitration ☐

I, Evan P. Lestelle, counsel for United States of America, do hereby certify that the above captioned civil action is ineligible for compulsory arbitration for the following reason(s):

☐ monetary damages sought are in excess of $150,000, exclusive of interest and costs,

☑ the complaint seeks injunctive relief,

☐ the matter is otherwise ineligible for the following reason

DISCLOSURE STATEMENT - FEDERAL RULES CIVIL PROCEDURE 7.1

Identify any parent corporation and any publicly held corporation that owns 10% or more or its stocks:

RELATED CASE STATEMENT (Section VIII on the Front of this Form)

Please list all cases that are arguably related pursuant to Division of Business Rule 50.3.1 in Section VIII on the front of this form. Rule 50.3.1 (a) provides that "A civil case is "related" to another civil case for purposes of this guideline when, because of the similarity of facts and legal issues or because the cases arise from the same transactions or events, a substantial saving of judicial resources is likely to result from assigning both cases to the same judge and magistrate judge." Rule 50.3.1 (b) provides that " A civil case shall not be deemed "related" to another civil case merely because the civil case: (A) involves identical legal issues, or (B) involves the same parties." Rule 50.3.1 (c) further provides that "Presumptively, and subject to the power of a judge to determine otherwise pursuant to paragraph (d), civil cases shall not be deemed to be "related" unless both cases are still pending before the court."

NY-E DIVISION OF BUSINESS RULE 50.1(d)(2)

1.) Is the civil action being filed in the Eastern District removed from a New York State Court located in Nassau or Suffolk County? ☐ Yes ☑ No

2.) If you answered "no" above:

a) Did the events or omissions giving rise to the claim or claims, or a substantial part thereof, occur in Nassau or Suffolk County? ☑ Yes ☐ No

b) Did the events or omissions giving rise to the claim or claims, or a substantial part thereof, occur in the Eastern District? ☑ Yes ☐ No

c) If this is a Fair Debt Collection Practice Act case, specify the County in which the offending communication was received:

If your answer to question 2 (b) is "No," does the defendant (or a majority of the defendants, if there is more than one) reside in Nassau or Suffolk County, or, in an interpleader action, does the claimant (or a majority of the claimants, if there is more than one) reside in Nassau or Suffolk County? ☐ Yes ☐ No

(Note: A corporation shall be considered a resident of the County in which it has the most significant contacts).

BAR ADMISSION

I am currently admitted in the Eastern District of New York and currently a member in good standing of the bar of this court.

☑ Yes ☐ No

Are you currently the subject of any disciplinary action (s) in this or any other state or federal court?

☐ Yes (If yes, please explain ☑ No

I certify the accuracy of all information provided above.

Signature: Evan P. Lestelle

Last Modified: 11/27/2017

EXHIBIT 4

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

[CAPTION]

Plaintiff, complaining of the ~~UNITED STATES OF AMERICA~~defendants, by ~~and through the undersigned~~his attorneys, ~~hereby~~THE BERKMAN LAW OFFICE, LLC, alleges for his complaint, upon information and belief, as follows:

INTRODUCTION

~~1. The United States brings this action for a temporary restraining order, preliminary and permanent injunctions, and other equitable relief pursuant to 18 U.S.C. § 1345, in order to enjoin the ongoing commission of criminal wire fraud in violation of 18 U.S.C. § 1343 and conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349. The United States seeks to prevent continuing and substantial injury to the victims of fraud.~~

~~2. Since at least 2016 and continuing through the present, Defendants, together with one or more co-conspirators, have used the U.S. telephone system to engage in predatory wire fraud schemes that victimize individuals throughout the United States, including individuals within the Eastern District of New York and significant numbers of elderly and vulnerable victims. Defendants are VoIP[1] carriers, and their principals, that serve as "gateway carriers,"[2] facilitating the delivery of millions of fraudulent "robocalls"[3] every day from foreign call centers and foreign VoIP carriers to the U.S. telecommunications system and ultimately to phones throughout the United States. The Defendants thus provide foreign fraudsters the means to access the U.S. telephone system, knowingly passing millions of fraudulent robocalls intended to deceive the recipient into: (1) answering or returning the call, and (2)~~

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

~~paying money to the perpetrators of the schemes.~~

~~3. Through these robocalls, fraudsters operating overseas impersonate government entities and well-known businesses by "spoofing"[4] legitimate phone numbers and sending recorded messages that are transmitted across the internet to telephones throughout the United States. These robocalls purport to be from federal government agencies, elements of foreign governments, and legitimate businesses, conveying alarming messages, such as that the call recipient's social security number or other personal information has been compromised or otherwise connected to criminal activity; the recipient faces imminent arrest; the recipient's assets are being frozen; the recipient's bank and credit accounts have suspect activity; the recipient's benefits are being stopped; the recipient faces imminent dep011ation; or combinations ·~~

~~1 VoIP stands for voice over internet protocol and allows users to place phone calls over a broadband internet connection.~~

~~2 As set forth in greater detail herein, "gateway caiTiers" are the first in a chain of VoIP carriers located in the United States that facilitate the delivery of foreign VoIP calls to recipients in the United States.~~

~~3 "Robocall" means a call made through an automat d process that places large volumes of telephone calls over the internet in order to deliver recorded messages, in contrast to calls placed one at a time by a live person.~~

~~4 The practice of making a false number appear on the recipient's caller ID is known as "spoofing." of these things all lies intended to induce potential victims to speak to the fraudsters. When individuals answer the calls or return voicemail messages, the fraudsters offer to "resolve" these• legal matters by immediate transfers of funds to settle the purported~~

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

~~legal obligation, or to hold the individual's assets only temporarily while the crisis resolves. In reality, the individual is neither under investigation nor in legal jeopardy, and the same threatening robocall was made simultaneously to thousands of other U.S. telephones.~~

~~4. Not only do Defendants deliver vast numbers of fraudulent robocalls every day, but they also participate in the fraudulent schemes by providing return calling services the fraudsters use to establish contact with potential victims. Robocall messages will often provide domestic and toll free call back numbers; potential victims who call these numbers connect to the overseas fraudsters, who then try to ext01i and defraud the potential victims.~~

~~5. Defendants profit from these fraudulent robocall schemes by receiving payment from their co conspirators for the services Defendants provide. Often, these payments consist of victim proceeds, a portion of which is deposited directly into Defendants' accounts in the United States, before the remainder is transmitted to the fraudsters overseas.~~

~~6. Since at least 2016 and continuing through the present, as a result of their conduct, Defendants and their co conspirators have defrauded numerous victims out of millions of dollars, including victims in the Eastern District of New York.~~

~~7. For the reasons stated herein, the United States requests injunctive relief pursuant to 18 U.S.C. § 1345 to enjoin Defendants' ongoing schemes to commit wire fraud in violation of 18 U.S.C. § 1343 and conspiracy to connp.it wire fraud in violation of 18 U.S.C. § 1349.~~[5]

~~[5] This case is one of two cases being filed simultaneously in which the United States~~

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

~~Department of Justice, for the first time, seeks to enjoin telecommunications companies from pruiicipating in robocalling fraud schemes pursuant to 18 U.S.C. § 1345.~~

1. The phenomenon of robocalls has become a scourge plaguing our society.

2. For years Americans have been constantly bombarded with robocalls seeking to draw them into all manner of fraudulent schemes with lies and deceit. Call recipients are told that their social security numbers will be "frozen" if they do not cooperate with a bogus investigator who needs money to be sent in immediately, that they will be arrested for money laundering or drug dealing, that they must provide their credit card or banking information, that their car warranties are about to expire, that they need to provide credit card information for cockeyed reasons, that there are tax liens against them, that they are going to be deported, and the list goes on. Many have been bombarded with pointless calls playing recordings in Chinese, Spanish, and other foreign languages they do not even speak.

3. The problem has become so severe that in 2018 when the Swedish Royal Academy of Sciences called New York University professor Paul Romer to inform him that he had won the Nobel Prize in Economics, he let the call go to voicemail thinking that only a telemarketing call could be coming in at such an early hour. He told the media "I didn't answer the phone because I've been getting so many spam calls. I just assumed it was more spam."

4. Millions of Americans have had their children woken up, had their dinner hour disturbed, have their work interrupted, have been unable to keep their phones on so their families could reach them for fear of having it ring at an inopportune time, have had to put important calls on hold to answer what turns out to be a spam robocall, and have otherwise have had their lives made miserable by spam robocalls.

5. The Defendants in this case are responsible for this scourge. Disregarding all laws,

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

ignoring complaints and warnings, and acting with a selfish quest for mammon regardless of the intrusive burden they placed on their fellow Americans, the Defendants deliberately facilitated hundreds of millions of spam robocalls, while hiding behind false telephone numbers and spoofed caller ID's.

6. In this action, plaintiff seeks justice on his own behalf, and on behalf of all the Defendants' other victims.

7. It is the plaintiff's hope that by imposing a financial cost on the defendants for the wanton aggravation they have caused to millions of Americans, the profit motive will be eliminated, similar conduct by others will be deterred, and Americans' quality of life can be improved.

THE **PARTIES**

~~8. Plaintiff is the United States of America.~~

8. At all times relevant to this complaint, the plaintiff, DOV ZEITLIN ("ZEITLIN"), is a natural person, resident of the State of New York, County of Kings.

~~1.~~9. Upon information and belief, at all times relevant to this complaint, Defendants Nicholas and Natasha Palumbo own and control Ecommerce National, LLC, doing business as TollFreeDeals.com and SIP Retail, LLC, also doing business as SipRetail.com (the "Palumbo Corporate Defendants"), which the Palumbos utilize in furtherance of the fraudulent robocall schemes. The Palumbos operate the Corporate Defendants from their home in Paradise Valley, Arizona, and on information and belief, the Palumbos operate SIP Retail as an alter ego of Ecommerce. From their home in Paradise Valley, Arizona, the Palumbos operate the Corporate Defendants as fraudulent enterprises.

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

~~2.~~10. Upon information and belief, at all times relevant to this complaint, Defendant Ecommerce is a~~n~~ corporation organized and existing under the laws of the State of Arizona. Ecommerce does business as TollFreeDeals.com, and will be referred to throughout this Complaint as TollFreeDeals. TollFreeDeals' principal place of business is located at the Palumbos' home in Paradise Valley, Arizona. Nicholas Palumbo is the Chief Executive Officer of TollFreeDeals and Natasha Palumbo is the Vice President of Business Development.

~~3.~~11. Upon information and belief, at all times relevant to this complaint, Defendant SIP Retail, LLC, also doing business as SipRetail.com ("SIP Retail"), is a corporation organized and existing under the laws of the State of Arizona. SIP Retail's principal place of business is located at the Palumbos' home in Paradise Valley, Arizona. Natasha Palumbo is the Chief Executive Officer of SIP Retail. SIP Retail provides VoiP carrier services for some of the same customers as TollFreeDeals, including foreign VoiP carriers that transmit millions of calls every week destined for the phones of residents of the Eastern District of New York.

12. Upon information and belief, at all times relevant to this complaint, Defendant Kaen resides in Nassau County, New York, in the Eastern District of New York. Kaen controls Defendants Global Voicecom, Inc., Global Telecommunication Services Inc., and KAT Telecom, Inc., which he uses in furtherance of the fraudulent robocall scheme. Kaen operates the Corporate Defendants as a single enterprise from his home in the Eastern District of New York. One or more of these Defendants also conducts business as "IP Dish."

13. Upon information and belief, at all times relevant to this complaint, Defendant Global Voicecom, Inc. is a New York corporation. The New York Department of State, Division of Corporations Entity Information database identifies Global Voicecom's principal executive office as being located in Great Neck, New York, in the Eastern District of New York, and Kaen

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

as the corporation's Chief Executive Officer.

14. Upon information and belief, at all times relevant to this complaint, Defendant Global Telecommunication Services Inc. is a New York corporation. Global Telecommunication Service's principal place of business is located in Great Neck, New York, in the Eastern District of New York.

15. Upon information and belief, at all times relevant to this complaint, Defendant KAT Telecom, Inc. is a New York corporation. KAT Telecom's principal place of business is located in Great Neck, New York, within the Eastern District of New York.

JURISDICTION

16. This court has jurisdiction over this action pursuant to 28 U.S.C. § 1331, 47, U.S.C. § 227, as well as 28 U.S.C. § 1367.

17. Venue lies in this district pursuant to 28 U.S.C. § 1391(b)(2)

CLASS ACTION ALLEGATIONS

18. This action is being commenced as a proposed class action, pursuant to Fed. R. Civ. P. 23.

19. The proposed class consists of all persons who received robocalls via the defendants' telecommunications services within the four years preceding the filing of this complaint.

20. This proposed class is so numerous that joinder of all members is impracticable.

21. There are questions of law or fact common to the class which predominate over any questions affecting only individual class members.

22. The claims of the representative plaintiff are typical of the claims of the class as a

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

whole.

23. The representative plaintiff will fairly and adequately protect the interests of the class.

24. A class action is superior to other available methods of the fair and efficient adjudication of the controversy.

THE UNDERLYING FACTS

Overview of Robocalling Fraud Schemes

A. Robocalling Fraud Targeting Individuals in the United States

~~9.~~25. ~~The~~Upon information and belief, the robocalling fraud schemes in which the Defendants are engaged share the same characteristics. Individuals at call centers located abroad, many of which are operating out of India, are bombarding the U.S. telephone system ~~daily~~every day with millions of robocalls intended to defraud individuals in the United States. Many of these- fraudsters impersonate U.S. government officials, foreign government officials, or well-known American businesses, in order to threaten, defraud, and extort money from robocall recipients. Robocalling technology, which allows fraudsters to send millions of calls per day all transmitting the same pre-recorded, fraudulent message, enables fraudsters to cast a wide net for elderly and vulnerable victims who are particularly susceptible to the threatening messages the fraudsters are sending. Even if only a small percentage of the recipients of a fraudulent call center's robocalls connect with potential victims, the fraudsters can still reap huge profits from their schemes.

~~10.~~26. ~~Foreign~~Upon information and belief, foreign fraudsters operate many different ~~scams~~schemes targeting individuals in the United States, but the Defendants' robocall schemes

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

include the following categories of impersonation scams:

a Social Security Administration ("SSA") Imposters: Defendants transmit recorded messages in which SSA imposters falsely claim that the call recipient's social security number has been used in criminal activity, the individual's Social Security benefits will be suspended, the individual has failed to appear before a grand jury and face imminent arrest, or the ~~recipient's~~individual's social security number will be terminated. When a call recipient calls back or connects to the fraudster, the fraudster claims to be an SSA employee and typically tells the individual to transfer substantial funds to the SSA for safekeeping until a new social security number can be issued, at which point the individual's funds purportedly will be returned.

~~a.~~b. Internal Revenue Service ("IRS") and Treasury Imposters: Defendants transmit recorded messages in which IRS imposters falsely claim that the call recipient has been implicated in tax fraud, the individual has avoided attempts to enforce criminal laws, the individual has avoided court appearances, or the ~~recipient~~individual faces imminent arrest. When a recipient calls back or connects to the fraudster, the fraudster claims to be an IRS

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

or Treasury employee and typically ~~directs~~tells the recipient to transfer funds to the IRS to resolve various fictitious tax and legal liabilities, or for safekeeping in order to avoid seizure of assets.

~~b.~~c. United States Citizenship and Immigration Services ("USCIS") Imposters: Defendants transmit recorded messages in which USCIS imposters falsely claim that the call recipient has failed to fill out immigration forms correctly, the ~~recipient~~individual faces imminent arrest or deportation, that the ~~recipient's~~individual's home country has taken formal action ~~against the recipient~~ that may result in deportation, or the ~~recipient~~individual has transferred money in a way that will result in deportation. When a call recipient calls back or connects to the fraudster, the fraudster claims to be a USCIS employee and typically tells the ~~recipient~~individual to pay various fees or fines to avoid immigration consequences.

d. Foreign Government Imposters: Defendants transmit recorded messages in which foreign government imposters, often in foreign languages, falsely claim to be from the U.S.-based consulate of a foreign government and that the call recipient faces problems with

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

immigration status or a passport. When a call recipient calls back or connects to the fraudster, the fraudster falsely claims that the individual must pay various fees or fines in order to avoid immigration consequences such as deportation.

e. Tech Support Imposters: Defendants transmit recorded messages in which fraudsters operating tech support scams impersonate various well-known tech companies such as Apple or Microsoft, and falsely claim that the call recipient has computer security problems that require assistance. When an individual connects with the fraudster, the fraudster instructs the individual to pay for fictitious tech support and computer security services, and to allow the fraudster remote access to the victim's bank accounts.

~~c. *Loan Approval Scams:* Defendants transmit recorded messages in which fraudsters operating loan approval scams impersonate a "lender" offering a great, guaranteed rate on a "pre-approved" loan. When a customer connects with the fraudster, the fraudster will emphasize that a poor credit history does not matter, all the call recipient has to do to secure the pre-approved loan is pay a one-time fee up front.~~

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

~~11.~~27. ~~These~~ b Upon information and belief, these robocalls are often "spoofed" so that they falsely appear on a victim's caller ID to originate from U.S. federal government agency phone numbers, such as the SSA's main customer service number, from local police departments, 911, or from the actual customer service phone numbers of legitimate U.S. businesses. These "spoofed" numbers are used to disguise the origin of the robocalls and the callers' identities, and to cloak them with the authority of government agencies or large businesses to induce potential victims to answer or return the calls. In reality, the calls originate from fraudsters operating abroad, and have no connection to any U.S. government agency or other legitimate enterprise.

28. Upon information and belief, individuals who answer or ~~return~~otherwise respond to these calls eventually speak to live fraudsters who tell the individuals lies intended to frighten and confuse them so that the fraudsters may begin to control their behavior and isolate them from authorities, friends, and family members. These lies often include that the individual's social security number or other personal information has been implicated in criminal activity, that the individual faces imminent arrest or deportation, and that the individual's assets are about to be forfeited to the government. Once an individual is overcome by fear and panic, the fraudsters keep them on the phone and offer reassurances that the individual's purported legal problems can be resolved through payment of money, or that the individual's money must be transferred for safekeeping to the government agency the fraudsters are impersonating. The fraudsters often claim that the victim's payment will be returned to them in the immediate future. In reality, once the fraudsters are convinced they have extorted as much money as possible from the victim, they drop all contact, leaving the victim without meaningful recourse. Fraudsters receive victims' money through retail gift cards, bank wires, cash payments, cryptocurrency transfers, and other

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

methods.

~~12.~~29. ~~Since~~Upon information and belief, since October 2018, the most prolific robocalling scam impersonating U.S. government officials-and one engaged in by Defendants-is impersonation, of the SSA. For example, a robocall sent to millions of phones in the United States in early 2019 contained the following message:

> Hello this call is from Department of Social Security Administration the reason you have received this phone call from our department is to inform you that there is a legal enforcement actions filed on your social security number for fraudulent activities so when you get this message kindly call back at the earliest possible on our number before we begin with the legal proceedings that is 619-[XXX]- [X:XXX] I repeat 619-[:XXX]-[X:XXX] thank you.

30. Upon information and belief, SSA received more than 465,000 complaints about fraudulent telephone impersonation of the Administration from October 1, 2018 through September 30, 2019. Losses associated with these complaints exceed $14 million. Similarly, the Federal Trade Commission ("FTC") reported that ~~during~~for 2018, its Consumer Sentinel database received more than 39,000 fraud complaints about SSA imposter calls, with estimated ~~victim~~ losses of approximately $11.5 million; for 2019, the FTC reported that SSA imposter call complaints rose to approximately 166,000 with associated losses of more than $37 million.[1] Complaint numbers

[1] Regarding government imposter fraud more broadly and not limited just to SSA imposters, the FTC's Consumer Sentinel database contains 255,223 complaints reflecting $128,479,054 in losses ~~of more than $37 million.~~[6] ~~Complaint numbers~~ for 2018, and 389,563 complaints reflecting $152,946,623 in losses for 2019.

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

substantially underrepresent the extent of the problem, because most victims do not report their losses to the government.

B. How Calls From Foreign Fraudsters Reach U.S. Telephones

31. Upon information and belief, the Defendants'~~The Defendants'~~ robocalling fraud schemes, which involve robocalls that originate abroad and target individuals in the United States, are all dependent on VoiP and related technology to create the calls. VoiP calls use a broadband internet connection~~—~~-as opposed to an analog phone line-to place telephone calls locally, long distance, and internationally, without regard to whether the call recipient uses a cellular phone or a traditional, wired phone. The robocalling fraud schemes also require U.S.-based telecommunications companies-referred to as "gateway carriers" to introduce the foreign phone traffic into the U.S. phone system. A foreign call center or telecommunications company that places VoiP calls to U.S. telephones must have a relationship with a U.S. gateway carrier. From the gateway carrier, most VoiP calls will pass through a series of U.S.-based VoiP carriers before reaching a consumer-facing "common carrier" such as AT&T or Verizon, and ultimately a potential victim's phone. One of the Defendants' roles in the fraudulent schemes is to serve as a gateway carrier for the fraudulent robocalls.

~~4.~~32. ~~Each~~Upon information and belief, each provider in the chain that transmits a VoiP call maintains records, primarily for billing reasons, of all of the calls that pass through it. These records include the following information: the date and time of the call, the destination number (intended recipient), the source number from which the call was placed (sometimes a

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

real number and sometimes a spoofed number), the name of the company that sent the call to the provider, and the downstream company to which the provider sent the call. These records are generated automatically as a call is routed through telecommunications infrastructure in a manner that achieves the lowest cost to transmit a given call, known in the industry as "least-cost routing." Calls may be traced through these records back to their gateway carrier, and thus to their foreign source. The telecommunications industry refers to this tracing process as "traceback."

~~13.~~33. Upon information and belief, tracebacks of many different robocalling fraud schemes have led to the identification of Defendants as a gateway carrier willing to transmit huge volumes of fraudulent robocalls into the country, despite clear indicia of fraud in the call traffic and actual notice of fraud.

Defendants' Ongoing Participation in Robocalling Fraud Schemes

~~14.~~34. Upon information and belief, since at least 2016, ~~and continuing through~~ the ~~present,~~ Defendants have knowingly provided U.S.-bound calling services to foreign fraudsters operating robocall scams, acting as a gateway carrier and passing robocalls into the U.S. telephone system by the millions. The Defendants are paid for each call they pass into and through the U.S. ~~phone~~telephone system. In addition, the Defendants have provided return-calling services to the fraudsters operating the robocall scams, for which Defendants are also paid, enabling the fraudsters to establish contact with unwitting individuals after the individuals are deceived by a robocall.

35. ~~There~~Upon information and belief, there is substantial evidence of the Defendants' knowledge of the fraudulent nature of the calls they transmit, including call records showing high percentages of short- duration, unanswered calls [7] passing through their systems by the millions; thousands of spoofed calls originating from overseas, purporting to be from "911"

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

and similar numbers; dozens of complaints and warnings from other telecommunications companies about fraud, spoofing, and short-duration "junk" calls; repeated warnings and inquiries from a telecommunications industry trade group about the fraudulent robocalls passing through the Defendants' system; and receipt of ~~payment from their foreign customers in the form of large, suspicious cash deposits by various individuals throughout the United States directly into Defendants' bank accounts.~~ numerous complaints from common-carrier telecommunications companies whose customers were victims of these fraud schemes.

A. Defendants Knowingly Introduce Fraudulent Robocalls into the U.S. Telephone System

36. Upon information and belief, in the telecommunications industry, high volumes of short-duration and unanswered calls are indicative of robocalls that are unwanted by the recipients, often because they are fraudulent. Defendants regularly transmit massive volumes of such calls. For example, a Government investigation has revealed a sample of more than 7.7 million calls that Defendant Global Voicecom routed through a single downstream VoiP carrier over 19 days in May and June 2019, months after Kaen's response to the FCC. Of those calls, approximately 86%, more than 6.6 million calls, were one second or less in duration, indicating exceedingly high levels of junk and fraudulent robocalls. Moreover, a small sample of approximately 330,000 of these calls was examined in greater detail; of these approximately 330,000 calls in that 19-day period, more than 270,000 (approximately 81%) were from source numbers (the numbers appearing on the recipients' caller IDs) identified as fraudulent robocalls. Similarly, of the more than 106,000 robocalls spoofing the SSA's toll-free customer service number in January and February 2019 that Defendant Global Voicecom transmitted into the United States, nearly 60% had a call duration of

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

less than one second, and another 38% were between one and 60 seconds in duration. During that same period in January and February 2019, Defendant Global Voicecom also ran through its systems thousands of calls spoofing 911, 1911, and 11911, with similar short call durations.

~~5.~~37. Upon information and belief, Defendants provide inbound VoiP calling to the United States telecommunication system (referred to in the industry as "U.S. call termination") to customers located both here in the United States and abroad. Defendants provide unrestricted VoiP calling, meaning they do not monitor or restrict the inbound calls a customer can place for either volume of calls or call duration. Defendants are paid for each call they pass into and through the U.S. phone system.

~~6.~~38. Upon information and belief, Defendants specifically market their services to foreign call centers and foreign VoiP carriers looking to transmit high volumes of robocalls to individuals in the United States. The TollFreeDeals website states "TollFreeDeals.com is your premier connection for call center and dialer termination. We are always looking for the best call center routes in the telecom industry. We specialize in short call duration traffic or call center traffic. We understand there is a need for it and we want to help you find all the channels you need!"

~~15.~~39. Upon information and belief, the FAQs on the TollFreeDeals website state, "Do you handle CC (Call Center)/Dialer Traffic? Yes-- unlike many carriers we will handle your dialer and call center VoiP termination minutes. If you are looking for USA Dialer, Canada Dialer, or Australia Dialer please fill out our online interop form to test our routes."

~~16.~~40. Upon information and belief, Defendants regularly transmit massive volumes of short duration calls. For example, over 23 days in May and June of 2019, TollFreeDeals

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

transmitted more than 720 million calls. Of those calls, more than 425 million, or 59% of the total calls, lasted less than one second in duration. In the telecommunications industry, high volumes of short-duration and unanswered calls are indicative of robocalls that are unwanted by the recipients, often because they are fraudulent. More than 24 million of those calls were placed to phone numbers with area codes in the Eastern District of New York. As Defendants' phone records show the ultimate destination number of every VoiP call they transmit, Defendants know they transmit fraudulent calls to potential victims in the Eastern District of New York.

41. ~~During~~ Upon information and belief, during May and June of 2019, the Palumbos facilitated the delivery of more than 182 million calls through TollFreeDeals from a single India-based VoiP carrier co-conspirator to phones in the United States. One thousand different source numbers (the number from which a call is placed, and that shows up on the recipient's caller ID) accounted for more than 90% of those calls. According to data obtained from a robocall blocking company about calls identified as fraudulent robocalls in 2019, 79% of those 1000 source numbers have been identified as sending fraudulent robocalls. Consequently, TollFreeDeals transmitted an estimated 143 million fraudulent robocalls on behalf of that single India-based co-conspirator during May and June of 2019. Of those calls, an estimated 20% were Social Security imposter calls, 35% were loan approval scams, and 14% were Microsoft refund scams. The remaining calls were a mixture of IRS imposter, U.S. Treasury imposter, miscellaneous tech support imposter and other schemes.

~~17.~~42. Upon information and belief, Defendants' knowledge of the fraudulent nature of the telephone calls they deliver to potential victims on behalf of their co-conspirators is also evidenced by the numerous complaints, inquiries, and warnings regarding fraudulent robocalls that

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

Defendants received from other telecommunications carriers and a telecommunications industry trade association since at least 2017. Despite receeiving these complaints, inquiries, and warnings, Defendants nevertheless continued to transmit massive volumes of fraudulent robocalls from their co-conspirators to potential victims in the United States.

43. ~~For~~Upon information and belief, for example, in May 2017, AT&T notified Nicholas Palumbo that it had traced back to TollFreeDeals robocalls received by its customers that spoofed phone numbers belonging to USCIS and the Office of the Inspector General of the U.S. Department of Homeland Security ("DHS-OIG"). AT&T informed Nicholas Palumbo that the callers who spoke to AT&T's customers impersonated U.S. Immigration Officers, and that AT&T had confirmed with USCIS and DHS-OIG that those agencies did not use any of the phone numbers at issue as a legitimate outbound caller ID. Nicholas Palumbo responded that the calls were transmitted to TollFreeDeals from an India-based VoiP carrier, and that he had blocked those two specific phone numbers. Blocking specific numbers is an ineffective means to stop fraudsters who are willing and have the ability to spoof any number as the caller ID number for their fraud calls.

44. ~~In~~Upon information and belief, in February 2019, AT&T notified Nicholas Palumbo that it had traced back 19 separate calls to AT&T customers that spoofed a USCIS phone number in order to "extort money from our customers." In Nicholas Palumbo's response to AT&T, he acknowledged that those calls were transmitted to TollFreeDeals from the same India-_based VoiP carrier that had transmitted spoofed USCIS calls in 2017. Despite repeated warnings from AT&T that this foreign VoiP carrier was transmitting fraudulent government-impersonation robocalls, the Palumbos continued transmitting VoiP calls on behalf of this customer through at

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

least as recently as June 2019.

~~18.~~45. ~~The~~Upon information and belief, the Palumbos have also received numerous warnings from telecommunications industry trade association US Telecom that both TollFreeDeals.com and SIP Retail have transmitted fraudulent robocalls, including government impersonation robocalls.

46. ~~From~~Upon information and belief, from May 2019 through January 2020, TollFreeDeals received 144 notifications from USTelecom that a fraudulent robocall had been traced back to TollFreeDeals. Of these notifications, 83 referenced SSA imposter fraud calls, 24 referenced Tech Support imposter fraud calls, ten referenced IRS imposter fraud calls, and one referenced USCIS impersonation fraud calls. Each of these emails were sent to Nicholas Palumbo at his @tollfreedeals.com email address. Each email stated that a suspicious call had been traced back to TollFreeDeals's network and provided the call date, time and the source and destination phone numbers, to allow TollFreeDeals to identify the specific call at issue in its call logs (referred to in the industry as "call detail records"). Each email also provided a link to USTelecom's web-based traceback portal, where further information was provided about the specific fraudulent call at issue, included a recording of the fraudulent voicemail message that was sent to the recipient's phone.

~~19.~~47. ~~In~~ Upon information and belief, in every case, either the email itself or the traceback pmial included a short description of the type of fraud at issue and the details of the fraudulent robocall campaign, such as:

> Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated voice claims suspicious activity on

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

> your social security number; press 1. Calls are from apparently random 8XX numbers or other geographic numbers. Call volume estimated at over a million transmitted spoofed US CIS calls in 2017.

~~per day. Because Caller ID changes with each call, blocking the ANI ["Automatic Number Identification"[8]] is not effective.~~

~~7.~~48. ~~After receiving each of these notifications from USTelecom, Nicholas Palumbo logged into the USTelecom portal and provided information regarding the customers of TollFreeDeals that had transmitted the~~ Upon information and belief, despite repeated warnings from AT&T that this foreign VoiP carrier was transmitting fraudulent government-impersonation robocalls, the Palumbos continued transmitting VoiP calls on behalf of this customer through at least as recently as June 2019.

49. Upon information and belief, the Palumbos have also received numerous warnings from telecommunications industry trade association US Telecom that both TollFreeDeals.com and SIP Retail have transmitted fraudulent robocalls, including government impersonation robocalls.

50. Upon information and belief, from May 2019 tluough January 2020, TollFreeDeals received 144 notifications from USTelecom that a fraudulent robocall had been traced back to TollFreeDeals. Of these notifications, 83 referenced SSA imposter fraud calls, 24 referenced Tech support imposter fraud calls, ten referenced IRS imposter fraud calls, and one referenced US CIS impersonation fraud calls. Each of these emails were sent to Nicholas Palumbo at his @tollfreedeals.com email address. Each email stated that a suspicious call had been traced back to

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

TollFreeDeals's network and provided the call date, time and the source and destination phone numbers, to allow TollFreeDeals to identify the specific call at issue in its call logs (referred to in the industry as "call detail records"). Each email also provided a link to USTelecom's web-based traceback portal, where further information was provided about the specific fraudulent call at issue, included a recording of the fraudulent voicemail message that was sent to the recipient's phone.

51. Upon information and belief, in every case, either the email itself or the traceback portal included a short description of the type of fraud at issue and the details of the fraudulent robocall campaign.

52. Upon information and belief, since 2017, significant numbers of fraudulent robocalls have been traced back to the Defendants and brought to their attention. For example, U.S. common carrier AT&T has notified Defendants on numerous occasions about fraud traced back to Defendants' operations. These notices include a November 16, 2017, email to IP Dish:

> The following calls to AT&T cell phone customers were received using the spoofed caller ID numbers of a non-working number at the US Department of Homeland Security headquarters. Callers impersonated US Citizenship and Immigration[ ] Services personnel and defrauded an AT&T customer of $1,450.... Pursuant to the customer and carrier network fraud protection provisions of the Telecommunication Act and the Telephone Records Privacy Protection Act (47 USC 222(d)(2)), could you provide the name(s) of your upstream carriers? We are tracing these calls to their source so they can be stopped.

53. Upon information and belief, AT&T sent similar emails about USCIS impersonation scams to Defendants Kaen and Global Voicecom in September 2017, November 2017, April 2018, and July 2018. Similarly, AT&T emailed Defendants about SSA and other

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

imposter robocalls on January 29, 2019:

> We have been receiving AT&T customers complaints about spoofing fraud from your network. In the first complaint calls are originating from a toll free number owned by the US Social Security Administration. Callers falsely claim to be US Government officials and attempt to extort money from our customers. We have verified this number is not out-pulsed as a legitimate caller ID by the real US Social Security Administration....
>
> In the second complaint calls are originating from the toll free number of DirecTV (AT&T). Callers falsely claim to be AT&T/DirecTV technical reps and social engineer remote access to our customer's computers in order to make fraudulent wire transfers from online banking applications....
>
> Could you provide the names and contact numbers of the parties that sent these calls to your network.

54. Upon information and belief, AT&T sent similar warning notices about SSA imposter calls to Defendants Kaen and Global Voicecom in February 2019 and May 2019.

55. Upon information and belief, another VoiP carrier that received call traffic from Defendants, Peerless Network, Inc., sent even more warning notices and inquiries to Defendants. For example, Peerless Network sent a warning notice about spoofed calls in September 2018 with a request that Defendants investigate and "take the appropriate action." Peerless Network sent approximately 12 of these warning notices between September 2018 and March 2019.

56. Upon information and belief, not only have other telecommunications companies provided warnings and notices to Defendants as a result of tracebacks, but a leading industry trade group, USTelecom, has done the same. For example, USTelecom traced back an August 19, 2019 robocall that originated from India and came through Defendant Global Voicecom as the

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

gateway carrier. The robocall was also routed through Defendant KAT Telecom. This robocall stated that there was "suspicious activity" associated with the individual's social security number. USTelecom provided the following warning notice in its correspondence to Defendant Global Voicecom on August 27, 2019:

> Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated voice claims suspicious activity on your social security number; press 1. Calls are from apparently random 8XX numbers or other geographic numbers. Call volume estimated at over a million per day. Because Caller-ID changes with each call, blocking the ANI is not effective.

57. Upon information and belief, blocking specific telephone numbers is an ineffective means to stop fraudsters who are willing- and have the ready ability-to spoof any number as the caller ID number for their fraudulent robocalls. For example, in January and February 2019, Defendants transmitted fraudulent robocalls spoofing 911, 1911, and 11911. Nevertheless, if the Defendants responded at all to these notices and warnings from other telecommunications-industry actors, they routinely responded that the "offending" number had been blocked, as though the spoofed telephone number and not the caller were responsible for the fraud.

58. Upon information and belief, similarly, USTelecom traced an October 3, 2019 robocall to Defendant Global Voicecom as the gateway carrier. This robocall also originated from India. USTelecom provided the following warning notice in its October 11, 2019 correspondence to Defendant Global Voicecom:

> Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Calls placed from specific numbers obtained by scammers, using an automated voice to

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

> inform called party that they are in trouble with IRS and will be arrested. Called party is instructed to call back to speak to an agent. .. We are using traceback to try to find the source(s) of the millions of outbound calls that are being made to initiate the scam.

59. Upon information and belief, USTelecom's records indicate that this robocall was transcribed in part as follows:

> This call is from Federal Tax and audit division of internal revenue services. This message is intended to contact you regarding an enforcement action executed by the US treasury intending your serious attention. Ignoring this will be an intentional second attempt to avoid initial appearance before a magistrate judge or a grand jury for federal criminal offense. This is a final attempt to reach you to resolve this issue immediately and to speak to a federal agent to call us back on 510-[XXX]-[XXXX]. I repeat 510-[XXX]-[XXXX].

60. Upon information and belief, USTelecom identified Defendants as the gateway carrier for foreign fraudulent robocalls on at least eighteen other occasions in the latter half of 2019 alone, each time providing similar warning notices about the nature of the scam robocalls. USTelecom's records indicate that on nearly all of these 2019 tracebacks, the scam robocalls came from the same company in India.

~~20.~~61. Upon information and belief, Defendants transmitted another group of fraudulent robocalls that· spoofed the phone number for a foreign government consulate in New York, New York. These calls conveyed foreign-language messages about problems with the individual's immigration status or passport. Like with SSA imposter robocalls and other U.S. government-imposter scams, individuals who returned the calls to the consulate imposters were told lies intended to frighten them and make them think there are imminent consequences for involvement

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

in criminal activity, and that funds must be transferred to the fraudsters to resolve the matters. Like with the SSA imposter scams, once the fraudsters are convinced they have extorted as much money as possible, they drop all contact with the victim. In 2018, the FCC traced this consulate imposter scam back to Kaen and IP Dish, who informed the FCC that the calls came from a Hong Kong entity that was making tens of thousands of calls per day. The FTC's Consumer Sentinel database reflects more than 1,000 complaints related to the spoofed phone number of the consulate. These complaints relate hundreds of thousands of dollars in victim losses. Defendants continue to conduct business of Defendants' customers with this Hong Kong entity more than a year later.

62. Upon information and belief, despite these notices and numerous others, Defendants continue to pass fraudulent robocalls into the U.S. telephone system to millions of U.S. telephones every day.

B. Defendants Provide Return-Calling and Toll-Free Services for Robocall Schemes

63. Upon information and belief, not only do Defendants knowingly pass fraudulent robocalls by the millions into the U.S. telephone system, but they also provide return-calling services to fraudsters so that potential victims can call them back. These toll-free and direct-inward-dial ("DID") telephone numbers and related services are provided in the robocall message as call-back numbers, and appear to be U.S. telephone numbers and thus enable fraudsters to further deceive individuals about the robocall's origin and the identities and locations of the fraudsters at the other end of the call. In reality, what appears to the individual to be a U.S. telephone number is actually a telephone number that Defendants register to an internet address designated by the foreign fraudsters. Thus, the DID and toll-free numbers can be used to ring telephones anywhere in the world.

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

64. Upon information and belief, while DID and toll-free numbers used for return-calling purposes cannot be "spoofed" like outgoing robocalls, the use of a U.S. DID or toll-free number in Defendants' robocalls schemes serves much the same purpose as spoofing-deception. The DID and toll-free services provided by Defendants use VoiP technology to direct potential victims' return calls from the United States to the foreign fraudsters' call centers. The Defendants have knowingly provided hundreds of these DID and toll-free numbers and associated calling services to foreign robocall fraudsters.

1. DID Numbers Used to Further Robocalling Fraud Schemes

65. Upon information and belief, like telephone numbers used to make U.S.-bound robocalls, DID numbers can be traced to identify their providers and users. This process was used to identify DID numbers provided by the Defendants for use in the fraudulent robocall schemes. For example, records obtained from one U.S. company demonstrate that it assigned 902 DID telephone numbers to Defendant Global Voicecom. Approximately 55% of these DID telephone numbers are associated with more than 28,000 complaints in the FTC's Consumer Sentinel database. One of the 902 DID telephone numbers appeared in a robocall sent to millions of U.S. telephones in early 2019:

> Hello this call is from Department of Social Security Administration the reason you have received this phone call from our department is to inform you that there is a legal enforcement actions filed on your social security number for fraudulent activities so when you get this message kindly call back at the earliest possible on our number before we begin with the legal proceedings that is 619-[:XXX]-[XXXX] I repeat 619-[:XXX]-[:XXXX] thank you.

66. Upon information and belief, at the time of the robocalls, this DID telephone

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

number was assigned to Defendant Global Voicecom, which used that DID telephone number to provide return-calling services to the overseas fraudsters. Individuals who return calls like these put themselves in a pool of likely victims, insofar as the individuals self-select through belief that the message was sufficiently credible to warrant a return call. Upon returning the call to 619-[:XXX]-[:XXXX], individuals were told that they were speaking to SSA agents, who offered to resolve the purported problems that prompted the call by way of immediate payment of funds. In reality, the person speaking to the individual was a fraudster, unaffiliated with the U.S. government.

67. Upon information and belief, beginning as early as September 2017 and continuing through the present, the U.S. company that assigned these 902 DID numbers to Defendants provided numerous warning notices about how the numbers were being used to perpetrate fraud. For example, that company provided the following warning notice to Defendant Global Voicecom on September 13,2017 and included the substance of several complaints about fraud:

> The DID: 847[XXXXX:XX] which we show assigned to you, is being used for fraudulent purposes. The US Treasury Department has provided us with a few complaints which are listed below. Because of the nature of the complaints, we have disabled this number on our network.
>
> I received a call from 484-[:XXX]-[:XXXX] claiming that I was a subject of Treasury Fraud. [T]hey said to call back at 847-[:X:XX]-[:XXXX]. The call was received on Friday September 8th at 4 pm. I live in Philadelphia, in the EST zone. They claimed I would be sued if I did not call back.
>
> I received a voicemail message with an automated recording claiming to be from the US Dept. of Treasury

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

> regarding tax fraud in my name. The call back number was 847-[XXX]-[:XXXX]. No one answered the return call. I recently submitted via mail my 3rd installment of2017 taxes, so I hope nothing has gone wrong in the process of receiving my payment. Is this a known scam number? Thank you.

68. Upon information and belief, the voice message states (Pre-recorded): "Treasury my badge number is 4874. The nature and purpose of this call is regarding an enforcement action which has been executed by the [U.S.] treasury department regarding tax fraud against your name. Ignoring this would be an intentional attempt to avoid initial appearance before the majesty does or exempt or enforce criminal offence. Before this matter goes to federal claim, court house, or before you get arrested. Kindly call us back as soon as possible. The number to reach us is 847-[X:XX]-[:XXXX], let me repeat the number 847-[X:XX]-[:XXXX]. Hope to hear from you soon before the charges are pressed against you. Thank you."

69. Upon information and belief, through the course of the ensuing years, Defendants continued to receive numerous similar warning notices about DID numbers and related services they provide. Defendants effectively ignored the warnings and never terminated the fraudsters' access to DID numbers for return calls.

70. Upon information and belief, in the course of a Government investigation, SSA OIG agents obtained from Global Voicecom call records for seven of the 902 DID numbers assigned to Defendant Global Voicecom that are associated with SSA imposter robocalls. According to Defendants' own records, Defendants provided these seven DID numbers to the same Indian entity that Defendant Global Voicecom identified to USTelecom as the gateway carrier for numerous government imposter scam robocalls.

71. Upon information and belief, these DID call records reveal that more than 10

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

million calls were placed in 2019 from more than 4.5 million unique phone numbers to the 902 DID numbers assigned to Defendant Global Voicecom. More than 240,000 of these calls were from area codes for the Eastern District of NewYork.

2. Toll-Free Numbers Used to Further Robocalling Fraud Schemes

72. Upon information and belief, records from the FTC demonstrate that Defendants Global Voicecom and Jon Kaen are associated with more than 1000 October 2019 SSA-imposter robocalls to the FTC's offices. These robocalls appeared to originate from a toll-free telephone number. Toll-free numbers work in a manner similar to DID numbers, but are structured differently by the FCC and telecommunications industry. Somos, Inc. is the FCC-designated national administrator of the U.S. toll-free calling system. Among other functions within the industry, Somos registers "responsible organizations" that are authorized to provide toll-free numbers to their customers and to register those numbers in the national registry that the industry uses to direct toll-free telephone traffic. On October 23 and 24, 2019, the FTC's offices received approximately 1,000 robocalls with the following recording:

> ...social security on an immediate basis as your social has been found some suspicious for committing fraudulent activities across the United State. Before we go ahead and suspend your social security permanently, we want you to call us back on our department toll free number at 877-[XXX]-[XXXX]. I repeat 8-877- [:XXX]• [XXXX]. Do not disregard this message, and call us back as soon as possible. Thank you.

73. Upon information and belief, the toll-free 877 number appeared on the FTC's caller ID as well as in the actual robocall message as the return-call number. On October 24, 2019, an FTC investigator contacted Somos to determine which responsible organization was associated with that toll-free number, which Somos duly provided. The FTC investigator then contacted that

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

responsible organization, who informed the investigator that the number was assigned to Defendants Global Voicecom and Jon Kaen.

74. Upon information and belief, that responsible organization provided numerous notices to Defendants concerning the toll-free numbers assigned to Global Voicecom and how they were being used to facilitate robocalling fraud, doing so 37 times between March 2019 and October 2019. For example, on April 8, 2019, the responsible organization emailed Defendant Global Voicecom: "We received a scam complaint on the number 888-[:XXX]-[:XXXX] and were asked to disconnect it. We dialed this number and found it was someone impersonating Microsoft, and is still connected." Similarly, on June 11, 2019, the responsible organization emailed Defendant Global Voicecom: "Please know that we have rec[ei]ved a serious complaint on TFN 888-[:XXX]-[:XXXX], which we see i[s] assigned to your account. This number was reported as a part of an "Amazon Customer Support Scam." On August 26, 2019, the responsible organization emailed Defendant Global Voicecom: "Please note that we have received reports that 877-[XxX]-[XXXX] is being used to spoof Bank of America. Can you please look into this, inform us of your results and take action if necessary?" To each of the dozens of notices, Defendants responded to the effect that the "offending" number has been blocked, as if the spoofed telephone number and not the caller were committing fraud, but never that they terminated the sources of the fraudulent robocalls.

~~72.~~75. The FTC's Consumer Sentinel reflects more than 1,400 complaints associated with the toll-free numbers assigned to Defendant Global Voicecom.

~~73.~~76. Upon information and belief, not only do Defendants knowingly pass fraudulent robocalls by the millions into the U.S. telephone system, but they also provide return-calling

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

services to fraudsters so that potential victims can call them back. These toll-free telephone numbers and related services are provided in the robocall message as call-back numbers, and appear to be U.S. telephone numbers and thus enable fraudsters to further deceive individuals about the robocall's origin and the identities and locations of the fraudsters at the other end of the call. In reality, what appears to the individual to be a U.S. telephone number is just a telephone number that Defendants register to an internet address designated by the fraudsters. Thus, the toll-free numbers can be used to ring telephones anywhere in the world.

~~21.~~77. ~~While~~Upon information and belief, while toll-free numbers used for return-calling purposes cannot be "spoofed" like outgoing robocalls, the use of a U.S. toll-free number in Defendants' robocalls schemes serves much the same purpose as spoofing--deception. The toll-free services provided by Defendants use VoiP technology to direct potential victims' return calls from the United States to the foreign fraudsters' call centers. The Defendants have knowingly provided toll-free numbers and associated calling services to foreign robocall fraudsters.

~~22.~~78. ~~All~~Upon information and belief, all toll-free numbers in the United States are administered by Somos, Inc., a company designated by the Federal Communications Commission ("FCC") as the national administrator of the U.S. toll-free calling system and its database. Among other functions within the industry, Somos registers "Responsible Organizations," that are authorized to provide toll- free numbers to their customers and to register those numbers in the national registry that the industry uses to direct toll-free telephone traffic. Defendants obtain toll-free numbers on behalf of their customers from one or more Responsible Organizations.

~~2.~~79. Upon information and belief, on July 31, 2019, an employee of a Responsible Organization sent the message below to Nicholas Palumbo via his @tollfreedeals.com email

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

address:

> Hello,
> We received a call yesterday (at 6 pm) that we didn't answer. Calling Number:+844[XXXXXXX]_Requesting to call back: 844-[XX:X:]-[XXXX] Please see the attached audio and screenshot of the voicemail transcript. Shut down this user immediately as it was associated with the customer account of [TollFreeDeals customer]. These types of scam calls are prohibited from our network and further fi·audulent calls from the same customer account will result in termination of said customer account. The number of 844-[XX:X:]-[X:X:XX] has been removed from your account in order to protect the integrity of our network.

80. ~~The~~Upon information and belief, the attached audio file of a voicemail message stated:

> tomorrow $399.99 is going to be deducted from your account for the remainder of your computer services. If you want to cancel the subscription, please press 1 to talk to our cancellation officer. Or you can call us back on our help line number l-844-[XX:X:]-[XX:X:X]. I'll repeat the help line number 1-844-[XX:X:]- [XXXX]. Thank you.

~~23.~~81. Upon information and belief, over the course of the next two weeks, employees of the Responsible Organization sent an additional six emails to Nicholas Palumbo, notifying him that the Responsible Organization was removing eight additional toll-free numbers from the accounts of two TollFreeDeals customers, because those numbers had been shown to be used in Tech Support impersonation scams and scams impersonating Amazon customer service. In response to each email, Nicholas Palumbo responded simply that he had let the customer of TollFreeDeals know.

82. ~~On~~Upon information and belief, on August 12,-2019, an employee of the

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

Responsible Organization emailed Nicholas Palumbo and stated:-

> Good afternoon Nick,
>
> I wanted to reach out to inform you that we have disabled the account of [TollFreeDeals customer] due to fraudulent complaints. Unfmiunately, we do get a lot of complaints about customers under your reseller account. Our first line of defense when issues like arise we deactivate the customer's account. I am informing you that if we do receive any additional complaints about any of your other customers under your re-seller account, we will be forced to deactivate your account.

83. Upon information and belief, Nicholas Palumbo responded "I let him know," then responded further, "I will be porting clients over[.] Can't take that chance." In the telecommunications industry, to "port a number" means to move an existing phone number from one provider to another. In effect, Nicholas Palumbo was stating that he planned to take the toll-free numbers registered to his customers through the Responsible Organization who had warned him about fraudulent calls, and move those same numbers to another provider on behalf of his customers.

Harm to Victims

~~24.~~84. Upon information and belief, Defendants' fraudulent schemes have caused substantial harm to numerous victims ~~throughout the United States~~, including many victims located in the Eastern District of New York. It is estimated that Defendants and their foreign co-conspirators defrauded victims out of millions of dollars per year through fraudulent robocalls and return-calling services. If allowed to continue, these losses will continue to rise and result in further harm to victims.

~~25.~~85. In addition to the massive cumulative effect of these fraud schemes on U.S. victims

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

~~throughout the United States~~, the harm can be devastating to individual victims. Victims have faced terrifying threats from fraudsters impersonating government officials and have lost substantial sums of money.

~~26.~~86. Defendants' fraudulent schemes are ongoing and wide-ranging. Absent injunctive relief by this Court, the Defendants will continue to cause injury to victims in this District and throughout the United States, and the victims' losses will continue to mount.

Government Action

87. The Government has filed two actions on these facts, *USA v. Palumbo, et al.*, EDNY case no. 20-cv-473, and *USA v. Kahen, et al.*, EDNY case no. 20-474.

AS AND FOR A FIRST CLAIM FOR RELIEF

88. Plaintiff repeats and re-alleges each of the foregoing allegations with the same force and effect as if more fully set forth herein.

89. The plaintiff, and each member of the proposed plaintiff class, has received numerous robocalls which, upon information and belief, were carried, processed, connected, placed, routed, and/or facilitated by the defendants and/or the agents, servants, employees, and related entities.

90. By their conduct, Defendants have violated the Telephone Consumer Protection Act ("TCPA"), 47 U.S.C. § 227.

91. The depth and breadth of Defendants' violation of the TCPA is astonishing, as it continued for years, involved hundreds of millions of calls, and continued despite multiple complaints, inquiries, and warnings, and thus could only have been deliberate conduct.

92. Defendants disregarded all laws and regulations, ignored do-not-call lists, and acted

Normal formatting = text present in both pleadings;
Underlined = text present in *Zeitlin* complaint but not in government action
~~Crossed out~~ = text present in government action but not in *Zeitlin* complaint

with complete lawlessness.

93. Pursuant to the TCPA, Plaintiff, and each member of the plaintiff class, may recover the greater of actual damages or $500, and the Court may, in its discretion, increase the amount of the award up to three times that amount.

94. The defendants are jointly and severally liable.

95. By reason of the foregoing, Plaintiff, and each member of the plaintiff class, is entitled to recover the full extent of his damages, in an amount to be determined by the jury at trial.

JURY TRIAL DEMANDED

96. Plaintiff demands a trial by jury of all issues triable to a jury.

WHEREFORE, the plaintiff demands judgment against the defendants in the amounts and for the relief requested herein, plus attorney's fees to the extent permitted by law.

Dated: Brooklyn, New York
January 29, 2020

Yours,

THE BERKMAN LAW OFFICE, LLC
Attorneys for the plaintiff

by: _____
Robert J. Tolchin

111 Livingston Street, Suite 1928
Brooklyn, New York 11201
(718) 855-3627

EXHIBIT 5

UNITES STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

Plaintiff,

-against-

NICHOLAS PALUMBO, NATASHA PALUMBO, ECOMMERCE NATIONAL, LLC d/b/a/ Tollfreedeals.com and SIP RETAIL d/b/a sipretail.com,

Defendants.

Case No.: 1:20-cv-00473-EK-RLM

DECLARATION OF NICHOLAS PALUMBO

NICHOLAS PALUMBO, under penalty of perjury, declares as follows:

1. I am a citizen of the State of Arizona with a home address in Paradise Valley, Arizona. I live here with my wife, Natasha Palumbo.

2. I am the President of Ecommerce National, LLC d/b/a/ Tollfreedeals.com ("Ecommerce"). I am a defendant in this action, as is my wife, who is the CEO of Sip Retail d/b/a sipretail.com.

I. Personal History

3. I was born in 1981 in Buffalo, NY. I am 38 years old. Throughout my life, I have been a self-starter and entrepreneur. My first job was at a landscaping company as a laborer in approximately 1999, this was summer employment in between schooling, after doing this for a few summers I started my own landscaping company one of the summers in between school semesters. I had one main client that ran into financial issues about the same time I went back to college, so the business ended at that time.

4. In 1999 I co-developed paintball informational website A-1Paintball.com. At the time we were trying to monetize the website via advertising. Ultimately a few years later

we decided to monetize the website via an online store front. We created the first version of A-1PaintballStore.com in 2002. It specialized in drop shipping paintball supplies to customers (drop shipping is business method where the retailer has no inventory and sends the products to the consumer directly from the warehouse supplier). The store sites were heavily constructed while I attended St. John Fisher College in Rochester, NY. In 2004 the store website was re-developed to be more efficient and database driven. At this time, we scaled the site to about 35,000 products. We did a major takeover in about 2007 of PaintballAdrenaline.com. This was a competitor of ours and we were able to streamline the operations with our ease of use order management system we created. I owned and operated this business until about 2008 when we sold the assets (primarily domain names).

5. I also have a self-taught background in internet marketing; for instance, I owned Shop4FishOil.com a website selling high grade supplements such as Dr. Sears fish oil. We created about 30 domain names over the years including GreenCoreFunding.com, ResidualAid.com, ManagementCosultingPro.com. In approximately 2011, I developed a custom CRM (customer relations management) software that helped me manage over 200 active leads at various stages of the telecommunications business single handedly.

6. After I moved to Arizona in 2009, I went to work for a company called RazorGator.com, an online ticket sales company located in Phoenix, AZ. I was their online marketing manager until the company went through a downsizing about 6 months into my employment.

7. In 2003, I first started to work in the telecommunications industry. I was selling mainly toll free numbers to businesses for a Las Vegas phone company named VersaPlanet. The CEO also taught me a lot about the wholesale communications business where we would introduce two intermediary carriers who were looking to find a partner to transfer calls

to or from. If a deal was reached, I received a commission per deal in a residual basis. After some setbacks, in 2003 I left the telecom industry for a few years and then returned in approximately 2010 where I started doing more brokering with the intermediary carriers.

8. I have never been charged with a crime. I have never been convicted of a crime. I have had a some very few parking and speeding tickets. There are no demerit points on my driving license.

9. In 2016, I married my wife, Natasha Palumbo. We have three children, two from Natasha's previous relationship and one three-year old daughter.

10. In 2016, I started my own intermediary carrier, Ecommerce. By intermediary carrier, I mean a telecommunications carrier that does business only with other carriers, not directly with callers or recipients of calls.

11. Sip Retail was incorporated as a sister company to Ecommerce. Both companies use the same equipment though they have separate FCC licenses. Like Ecommerce, Sip Retail is an intermediary carrier. This means it channels all calls carried over its platform to other intermediate carriers and does not do business directly with callers or recipients of calls.

II. Ecommerce and the VOIP Industry and Technology

A. About the industry.

12. Since internet connections became fast enough to connect audio – around the 2000s – and broadband connections became affordable, the "Voice over Internet Protocol", or "VOIP" technology started to take root. This technology changed the telecommunications industry, primarily by allowing smaller players to compete with large common carriers such as AT&T. This resulted in better technological solutions for the customers and more competition. The barrier to entry were drastically lowered; it is possible to set up a basic intermediary carrier with around $10,000 in initial investment.

13. Such a carrier, known as "intermediary carriers" or "wholesale carriers" do not themselves place calls – they connect other people's calls over the Internet. There are thousands of intermediary carriers that operate in the U.S. alone and even more overseas.

14. VOIP Calls are routinely routed through multiple carriers before they reach their destination; a single call may go through more than a dozen carriers before it is connected. It is extremely rare for an originator – the person who makes the call – to be connected to the recipient – the person who receives the call – by only one carrier. This multi-tiered web of linked intermediary carriers is normal and ensures competition for low connection fees.

15. The system works as follows: intermediary carrier A is paid money from intermediary carrier B to connect a call coming from carrier B through carrier A's system. Here, carrier B is carrier A's "client," carrier A is carrier B's vendor. If the call travels the other way – i.e. if carrier A wants to route a call through carrier B's system – then the terms are reversed and the money flows in the other direction. It is normal for carriers to be both vendors to and clients to each other.

B. Types of Calls in the Industry

16. The current case brought by the United States focuses on automated telephone calls commonly referred to as "robocalls." There are numerous legitimate uses of robocalls. For example, the Telephone Consumer Protection Act ("TCPA"), a law directed at countering fraudulent robocalls, contains an explicit exception for robocalls made to collect debts. Such calls are legal. In addition, many companies use robocalls to give reminders to their customers. For example, pharmacies use robocalls to alert clients when their medication is ready for pickup; doctors' offices use robocalls to remind patients when their appointments are; law offices use robocalls to reach out to potential class members in class-action lawsuits; the

government uses them to distribute school closing announcements; utility companies notify customers of service interruptions. This is especially useful with older consumers who are not well-versed with text messaging and email.

17. Call centers located abroad place calls into the U.S. Call centers have many legitimate uses in the modern industry. For example, a call center may engage in direct sales, which is a legal use of the telephone network. In addition, many companies when offering technological or services support have opted to use call centers abroad. While previously a consumer would have to call the customer support line and wait for a representative to become available, frequently companies (including Amazon) will let the customer "book" a call online and call the customer once a representative becomes available to avoid wasting the customer's time on the phone. In addition, political and other polling enterprises use call centers to ask individuals whom they would vote for. Political polls are labor intensive, and it is unsurprising that the political rating companies have long ago outsourced their call centers to locations outside the U.S.

18. Frequently, robocalls and call center traffic is mixed. A call may start with a prerecorded offer or reminder followed by the words "to be connected with an operator, press 1."

19. All of these calls, both robocalls and call center calls, often result in very short calls. This may be because the reminder about one's prescriptions only takes a few seconds; or it may be because recipients do not want to talk to a direct sales caller or give their opinion on politics.

20. Many intermediary carriers also provide toll-free numbers to their clients. This is legal and normal in the VOIP industry. Toll-free calls are beneficial in numerous contexts, including as an inducement to response in direct marketing.

C. Fraudulent Calls and How They Are Dealt With

21. Naturally, all of these – robocalls, call center traffic and mixed robocalls/call centers – can be exploited by con-artists and thieves. Robocalls can be used to defraud and deceive. Unfortunately, an intermediary carrier cannot distinguish between fraudulent and legitimate calls as they pass through their system.

22. Due to this industry structure, intermediary carriers like Ecommerce do not have contact with the original callers or the eventual recipients of calls. Usually a call originates many clients prior and is picked up many vendors later. The carriers do not know the content of the calls.

23. The system that Ecommerce and Sip Retail employ only reads the signal-level information, i.e. the meta-data of a call. This includes the call number (real or spoofed), the duration, the carrier it arrives from, etc. Our system – like most systems in the industry – does not include the actual transmission of the data packets of the call, i.e. the spoken words on the call. Put differently, even if we wanted to, we could not listen to individual calls. Any carrier that had the ability to listen to calls and did so would violate numerous privacy laws. In short, there is no way for a carrier to know what's in a call.

24. To stop fraudulent calls, carriers must rely on the complaints system. Such complaints are received from three sources: Common carriers (such as AT&T) and other intermediary carriers, USTelecom (a nonprofit trade and lobbying association for the U.S. broadband and communications industry) and Somos (a company designated by the Federal Communications Commission ("FCC") as the national administrator of the U.S. toll-free calling system and its database).

25. Once an intermediary carrier receives a complaint, it can and must review the phone number associated with the complaint. It must then alert the client from which it

received that call on that line; it will usually also block that number. The alert to the client operates as a follow-up complaint; the client will do the same thing on its network. This way the complaint and the problematic call can be traced to its source, where the fraudulent originator can be blocked. To the best of my recollection, that is what I did every time Ecommerce received a complaint.[1]

26. It would make no sense to block all calls from a client upon receipt of a complaint relating to one number from that client. That approach would be both over- and under-inclusive. It would be underinclusive because it would be pointless – the client (another carrier who would not be aware of the bad calls on its system) could simply route the calls through a different intermediary carrier. The approach is overinclusive, because it would take only a few hundred complaints to have all intermediary carriers block each other, essentially preventing any calls from being connected. There is no guideline, regulation, best practice, handbook, or industry standard that requires that an intermediary carrier must shut down an entire client when it receives a complaint about some of its numbers.

27. I have reviewed the USTelecom Industry Traceback Group Handbook on "Policies and Procedures" dated January 2020. This handbook was apparently published after this case started; I had not received a copy before. I received a link to the online publication of the handbook from a friend in the industry. The handbook prescribes exactly the methods outlined above – that carriers need to cooperate to trace the source of a fraudulent call once they are alerted through a complaint. The handbook does not require carriers to block other carriers.

28. The handbook also defines a "Non-Cooperative Voice Service Provider" as a "voice service provider that does not follow the best practices contained herein (pages 8-11)

[1] In fact, after this action commenced and TRO was in place, I terminated the account of one client as required by the TRO. The client emailed me and wanted to know the phone number that had caused the problem so that the issue could be addressed on the client end as well. A copy of that email exchange is annexed hereto as Exhibit 1.

and does not cooperate with Cooperative Voice Service Provider(s) or USTelecom on Tracebacks of Suspicious Traffic." The handbook further states that Non-Cooperative Voice Service Provider will receive warnings that they are being labelled "non-cooperative." I never received such a warning. The handbook is Exhibit 3 to the declaration of John Dalrymple.

29. The Government complaint makes reference to calls purporting to operate from "911." This happened, and as soon as we received notification that some calls purported to originate from 911, we blocked all such calls in May 2016. Thereafter the block expired, we extended it for as long as possible, which was until 2099.

D. About Defendants' Switch

30. As states above, we have no means to monitor whether a call that passes through our platform is a robocall, or a call center call, or a personal or business call.

31. The system that we use is entirely online; it is a SAAS ("software as a service") model. The platform we use is called SipNavigator. We lease the software and access to the platform. The cost of leasing SipNavigator is variable and decreases with the amounts of calls connected. At our peak, we had 38,000 phone lines, which cost $0.80 per month per line per month. The entire system, software and hardware together, is known as a "switch".

32. Our customers include small and medium-sized intermediary carriers. None of our customers are call originators, i.e. none of them are call centers or consumer members the public. The following list is a representative sample of our clients and vendors.

a. Yodel Voice, a large, well-established and reputable intermediary carrier in California.

b. Blue Tone Communications, a Rochester, NY-based intermediary carrier. Blue Tone also develops VOIP technology and software for other carriers.

c. Talkie Fiber, a carrier that specializes in connecting home users and business users with high speed internet. They are currently laying glass fiber cables in the Maryland area.

d. TouchTone Communications, a carrier based out of Whippany, NJ. This is a privately-owned facilities-based, full service telecommunications carrier and reseller.

e. Modok Telecom, based in California. This carrier specializes in working with small business and enterprise scale companies.

f. MashTelecom, which operates out of Montreal, Quebec, Canada.

g. XenCall, which operates out of Vancouver, BC, Canada.

33. In addition, Ecommerce is an eco-friendly company. As shown on our website, we have focused on water and energy sustainability to conserve water and electricity. I have always been an environmentalist and protecting the environment is a passion of mine.

E. Complaints

34. The Government claims there were "numerous complaints, inquiries, and warnings regarding fraudulent robocalls that Defendants received…" (Compl. ¶ 30). However, the evidence of such complaints is particularized, and the Government *nowhere* asserts that we ignored any complaint. The Government relies on the following isolated instances:

35. **May 2017, AT&T notification** (Compl. ¶ 31, Ralston Decl. ¶ 39). The Government admits that we blocked the relevant numbers over which complaints had been received. The Government argues that "[b]locking specific numbers is an ineffective means to stop fraudsters" (Compl. ¶ 31), but it does not allege that this opinion was communicated to us at the time or that it is an accepted industry view – neither is true. In addition, we did more than just block the number; we also notified the client, which is the standard in the industry. As a result,

the client took further action to block/remove a client on their switch. If any additional complaints came in, Ecommerce would reach out to the client for further client reduction on the wholesale carriers end.

36. **February 2019, AT&T notification** (Compl. ¶ 32). The Government refers to 19 calls that were allegedly fraudulent originating from a specific client. 19 problematic calls constitute only 0.000007% of the overall amount of calls connected that month or one in 14 million calls.[2] Also, we blocked the calls and notified the carrier per standard procedure.

37. **Vague references** to "numerous warnings" and "repeated warnings" (Compl. ¶ 33, Ralston Decl. ¶ 7). It is hard to respond to an allegation that is so unspecific. Similarly, the Government claims that we "received many notices, inquiries, warnings, complaints, and subpoenas concerning fraudulent robocalls" (Ralston Decl. ¶ 29). It is notable that the Government nowhere argues that any complaint was ignored.

38. **US Telecom notifications** between May 2019 and January 2020 (Compl. ¶¶ 34-36, Ralston Decl. ¶ 37). These 66 notifications[3] over a 9-month period average 7 complaints per month. We connected on average over 450 million calls per month in 2019. This means that on average 0.00000175 percent, or fewer than 1 in 60 million of all calls transmitted by us were flagged as questionable. The Government admits that *none* of these complaints were ignored by defendants (Compl. ¶ 35).

39. The Government, however, fails to mention the actions we took in response to each, which included each time communicating with the client-carrier that originated the problematic calls to follow the calls to their source. The Government claims that "Defendants

[2] The Government throughout claims that few complaints are indicative of a broader problem and that most fraudulent calls are not reported (Compl. ¶¶ 5, 19). This may be true, however, we cannot – and should not be expected to -- block calls that they have no information about.
[3] The Complaint refers to 144 notifications; however, a later-filed declaration (docket no. 8) clarified that only 66 notifications existed. This misrepresentation was repeated in the declaration of Marcy Ralston (Ralston Decl. ¶ 37).

blocked the single source number identified in the each [*sic*] email." (Ralston Decl. ¶ 33). That is a half-truth, since we worked with the client to solve the problem each time; which is also the course of action recommended by the USTelecom handbook.

40. **Complaints from Somos**, an FCC company that administers toll-free calls (Compl. ¶¶ 41-43). The Government alleges that a handful of toll-free numbers had been associated with fraudulent conduct. It admits, however, that we responded and dealt with each complaint ("In response to *each* email…" Compl. ¶ 42). The Government states that we "simply" made the client aware of the complaint, which is the most reasonable way of dealing with complaints. Though the Government insinuates that this was an insufficient response, it does not allege that any dissatisfaction with this response was communicated to us. It wasn't. Nor does the Government refer to any law, regulation, rule, or industry standard that prescribes a different action and none exists.

41. **Porting over.** The Government finally claims that when we stated that we would "port over" a problematic number, we were moving the problematic number to another carrier, ignoring the complaint (Compl. ¶ 43, Ralston Decl. ¶ 54). The argument has no merit. If we wanted to ignore complaints, we would not inform regulators of their violation.

42. The meaning of my statement that I will be "porting clients over" lies the use of the plural – "clients". The vendor Teli.net complained about *two* of our clients and threatened to close down all connections with all of our clients, including clients for whose activities we never received any complaints. The statement "I will be porting clients over" referred to the clients we had *other than* the two targeted by the complaint; it indicates that I was planning to move those other clients to a different vendor; thus if the complaining vendor were to shut down our connection to the vendor, our clients' call services would not experience any

interruptions. This was precisely the opposite of furthering fraudulently activity; the Government has what we were doing backwards.

F. Payments and Accounts Receivable

43. Our clients usually pay through various means – bank transfers, checks, paypal, credit card, and other online payment portals. I learned early as an entrepreneur that it is important to be user-friendly when it comes to clients.

44. We send out invoices to our clients weekly. In response, clients usually either pay the amount on the invoice exactly, or they run a balance with Ecommerce. The expectation is that the balance is positive and that payments are made to replenish their accounts. Sometimes a balance goes negative; in those cases, I contact the client and ask for additional money. Communications with clients is usually by email or text messaging through one or more messaging applications.

45. The money arrives at our accounts receivable bank account at Chase bank. Once there is a sizable amount of money in the account, it gets moved to the Ecommerce business expenses account, which is also at Chase bank. We pay our vendors and taxes and other business expenses out of that account. We try to avoid having a large balance in the accounts receivable account because the account details are given out to every client. The account is therefore to some extent vulnerable as a target for thieves who might impersonate us to the bank and move money out of the account.

46. The Government complaint refers to payments made to our Wells Fargo account. This account was set up for one client who had difficulty with Chase bank. I thought this was appropriate and established the account. The payments to this account made up less than 4% of our overall revenues.

47. The payments were made as with the other clients that carried a receivables balance. Copies of the Wells Fargo bank statements are annexed hereto as Exhibit 2. Copies of the invoices to that client are annexed hereto as Exhibit 3. Based on the statements I did not know where the payments had been made.

48. At various points in 2019, I communicated with Michael Rauch, our business bank representative at Chase banks about cash payments. He did not indicate that there was anything suspicious about the cash payments or that businesses should be wary of cash payments. Based on my interaction with him, we assumed that there was nothing to worry about concerning cash payments. Copies of the text messages with Mr. Rauch are annexed hereto as Exhibit 4.

49. I have never transmitted monies to India.

50. It is alleged that all these payments were payments of less than $10,000. That is incorrect, see Exhibit 2, page 8 (showing a $10,000 deposit on "8/2").

G. The Bracken Declaration

51. In his declaration, agent Samuel Bracken claims that between "May 28, 2019 through September 11, 2019, [defendants' Wells Fargo] account received nineteen cash deposits totaling $130,250.00. These deposits occurred in locations across the United States, including in Minnesota, South Carolina, Florida, Alabama, and New Jersey. None of these cash deposits occurred in Arizona, the principle [*sic*.] location of business for Ecommerce National." (Bracken Decl. ¶ 3).

52. The explanation for such deposits, however, shows no nefarious purpose – it appears that agents for two of our *customers* are located in U.S., and their deposits in U.S. currency were in payment for legitimate services that were duly invoiced. For example, the invoices for the client who deposited money into the Wells Fargo account are annexed hereto as

Exhibit 3. The other client made payments into the Chase accounts receivable account. Both clients are based overseas and apparently preferred to make their payments in this manner, which despite Bracken's innuendo, is not illegal.

53. We had no knowledge of the fact that these deposits were made in various states – the Wells Fargo bank statements does not identify the location of the deposits (Exhibit 2). It evidently took the resources of the Government to determine a fact that was not readily ascertainable by us.

54. The Bracken declaration adds that defendants transferred the monies to Chase bank (id. ¶ 4), claiming this is somehow nefarious (id. ¶ 5). However, the Chase bank accounts are simply our operating accounts out of which we pay our vendors and taxes. There is nothing nefarious in having an account for the receipt of payments on accounts receivable and one or more separate operating accounts for business expenses. Attached as Exhibit 5 are sample bank statements from Chase for both the account receivable and expenses accounts.

55. The Bracken declaration lists seven indicia that are allegedly associated with fraudulent activity (¶ 5) but fails to link any of them with the accounts. To do so would undermine the Government's argument since they can be readily explained:

- "out-of-state, anonymous cash deposits in multiple states" – As explained, we had no means of discovering the locations of the deposits.
- "rapid cash withdrawals for amounts similar to cash deposits" – We needed the money to pay bills; the Wells Fargo account was also far more public and vulnerable to attack by malefactors.
- "use of counter deposit slips" – The Government does not argue that this applies.
- "individual deposits and withdrawals intentionally under $10,000 (structuring)" – The Government does not, and cannot, argue that the amounts were *intentionally* made of a certain amount to hide them from scrutiny. In any case, the allegation is false; at least one deposit was $10,000 and thus subject to reporting [See Ex. (bank statement)].

- "limited account credits besides cash deposits (i.e., no payroll, wire transfers)" – as outlined *supra*, the Wells Fargo account was an accounts receivable account, not the expense account for our business.

- "no legitimate business purpose evident" – We have been in business for many years without any criminal record. To suggest that there is no legitimate business purpose is untrue.

- "deposit activity greater than expected income" – The Government does not state what the expected income would be, by how much it was exceeded, and how it would be calculated. Agent Bracken's listed experience does not include any indication that he has accounting experience sufficient to make this assessment. It is in any case inaccurate – the deposits were made in response to weekly invoices.

56. To the extent the Government insinuates – it stops short of making the argument outright – that these payments were made by victims as opposed to clients; the argument has two problems. First, there is no evidence in support – the Government is apparently unable to connect any payment to any alleged victim, and as shown, the transfers were made by legitimate clients. Second, we have never transmitted monies to India (or elsewhere abroad).

H. Other Points

57. I have been shown the Government's proposed preliminary injunction; a copy is annexed hereto as Exhibit 6. The terms are such that it would require us to shut down all clients. If this preliminary injunction is granted, Ecommerce and SipRetail will go out of business for good. In addition, if the preliminary injunction is in effect, there will be no need for a permanent injunction since it would be impossible for our business to recover from such a shutdown.

58. All of our business is with other intermediary carriers and to our knowledge none have committed fraud. None of the carriers with who we do business have been joined as defendants in this case. Other than through complaints, from third parties such as from

US Telecom, I have no knowledge of any calls carried over our platform that were fraudulent in nature.

III. The Events of January 28, 2020

59. On January 28, 2020, I was about to take my three-year old daughter to preschool at 8:30 a.m. The doorbell rang; I answered the door with my daughter in my arms expecting to see an Amazon delivery person.

60. Instead, approximately a dozen armed federal agents and local police were standing at the gates of my property. They had their guns pointed at me and my daughter. I was terrified.

61. I was instructed by the agents to put down my daughter, raise my hands over my head, turn around and walk backwards toward the agents. I complied. My daughter ran to her mother who was in the house.

62. The agents then handcuffed me and proceeded to execute two search warrants at our property. They took computers and records.[4] I was handcuffed and instructed that I could not leave; however, I was told that I was not under arrest. I have since learned from my attorneys that this was incorrect and that I was under *de facto* arrest.

63. After the agents searched my house, I was advised I could remain silent. Nevertheless, I proceeded to speak with the agents and explain our business and technology. While this may not have been the action that most lawyers recommend to their clients, I had no attorney at the time to advise me and I felt – and continue to believe – that I had nothing to hide since I had done nothing wrong. I have always been a law-abiding citizen, and always believed

[4] Though it was represented to me that these would be returned to me shortly, that has not yet happened. As a result, we have been unable to prepare our taxes for 2019.

that law enforcement acted in the interests of justice. I spent several hours speaking to the agents and answering their questions.

64. To this day, I have not been arrested (except during when our house was raided, and I was told I could not leave) or charged with any crime.

65. In the days and weeks following January 28, 2020, our three-year-old daughter has exhibited abnormal and new behavior, including extreme fearfulness and anxiety whenever a parent would not be in sight, and an inability to sleep without lights on. These are new and troubling behaviors; prior to this incident, she was a normally-developing child. We are considering finding a therapist for our daughter who specializes in early-age trauma.

66. On that same day, our accounts were frozen and about $180,000 was forfeited from our Chase banks accounts. We received nothing in writing that explained these actions or that stated at whose request or authority it was done even though we requested such basis from the government. Our bank was equally unhelpful and would not provide any information.

67. In addition, around $1-2,000 was forfeited from our Wells Fargo account; we were given a warrant for this action.

Dated: Paradise Valley, Arizona
February 25, 2020

Nicholas Palumbo

4840-4680-1846, v. 1

Gmail **Theodor Bruening <brueninglawyer@gmail.com>**

Re: Zeitlin v. Palumbo et al.

1 message

Robert Tolchin <rtolchin@berkmanlaw.com> Sun, Apr 12, 2020 at 4:07 PM
To: Theodor Bruening <brueninglawyer@gmail.com>

Theo,

Now I received it. I had not received it before.

I'm wondering if you would be amenable to having a conversation about this motion. Before we talk, though, I'd like to be clear that the conversation would be subject to FRE 408 privilege. Basically, I want to be able to talk frankly with you without either of us being concerned that the other will include the content of the discussion in any submission to the court.

Please advise.

Robert J. Tolchin, Esq.
THE BERKMAN LAW OFFICE, LLC
111 Livingston Street, Suite 1928
Brooklyn, New York 11201
718-855-3627

On Sun, Apr 12, 2020 at 10:12 AM Theodor Bruening <brueninglawyer@gmail.com> wrote:

> Robert: Below is a sharelink that allows you to download the attachments from my previous email. Please let me know if you have any issues with that. In addition, a set of hard copies will be delivered tomorrow by USPS to the address in your email signature, i.e. to 111 Livingston Street. If there is a more convenient address, please let me know and I will send another set to that address.
>
> Sharefile: https://drive.google.com/drive/folders/15zqEfV2rSo5BWqvyQXJnhu329OhaHoAb?usp=sharing
>
> Kind regards,
>
> Theo
>
> > On Apr 12, 2020, at 1:33 AM, Robert Tolchin <rtolchin@berkmanlaw.com> wrote:
> >
> > No attachments received
> >
> > Robert J. Tolchin, Esq.
> > THE BERKMAN LAW OFFICE, LLC
> > 111 Livingston Street, Suite 1928
> > Brooklyn, New York 11201
> > 718-855-3627

On Fri, Apr 10, 2020 at 3:48 PM Theodor Bruening <brueninglawyer@gmail.com> wrote:

> Robert: A few minutes ago I sent you an email with several attachments, see below. Please let me know if you did not receive it and I can send the attachments again in individual emails. Many thanks.
>
> Kind regards,
>
> Theo
>
> On Fri, Apr 10, 2020 at 3:35 PM Theodor Bruening <brueninglawyer@gmail.com> wrote:
>
> > Robert: Please see attached. A hard copy is being sent today.
> >
> > Kind regards,
> >
> > Theo